Avira Internet Security

Manuel de l'utilisateur





Marques et copyright

Marques

Windows est une marque déposée de Microsoft Corporation aux États-Unis et dans d'autres pays.
Tous les autres noms de marques et de produits sont des marques ou marques déposées de leurs propriétaires respectifs.
Les marques protégées ne sont pas désignées comme telles dans le présent manuel. Cela ne signifie pas qu'elles peuvent être utilisées librement.

Remarques concernant le copyright

Des codes de fournisseurs tiers ont été utilisés pour Avira Internet Security. Nous remercions les détenteurs des copyrights d'avoir mis leur code à notre disposition.
Vous trouverez de plus amples informations sur le copyright dans l'aide de Avira Internet Security sous « Third Party Licenses ».



Sommaire





1. Introduction

Avec votre produit Avira, protégez votre ordinateur contre les virus, vers, chevaux de Troie, logiciels publicitaires et espions, et de tout autre risque. Ce manuel aborde de manière simplifiée les virus, logiciels malveillants et programmes indésirables.

Le manuel décrit l'installation et l'utilisation du programme.

Sur notre site Web, vous pouvez trouver différentes options et autres informations :

http://www.avira.com/fr

Sur le site Web d'Avira, vous pouvez :

- accéder aux informations concernant les autres produits d'Avira
- télécharger les derniers produits d'Avira
- télécharger les derniers manuels des produits au format PDF
- télécharger les outils de support et de réparation gratuits
- utiliser la vaste base de connaissances et les articles FAQ détaillés pour la résolution des problèmes
- accéder aux coordonnées du support en fonction des pays.

Votre équipe Avira

1.1 Symboles et mises en page

Les symboles suivants sont utilisés :

Symbole / Désignation	Explication
✓	Se trouve devant une condition à remplir avant d'exécuter une manipulation.
▸	Se trouve devant une manipulation que vous effectuez.
↳	Se trouve devant un résultat qui découle de la manipulation précédente.
Avertissement	Se trouve devant un avertissement en cas de risque de perte critique de données.



Remarque	Se trouve devant une remarque contenant des informations particulièrement importantes ou devant une astuce qui facilite la compréhension et l'utilisation de votre produit Avira.

Les mises en page suivantes sont utilisées :

Mise en page	Explication
Italique	Nom du fichier ou indication du chemin.
	Éléments de l'interface logicielle qui s'affichent (par ex. zone de fenêtre ou message d'erreur).
Gras	Éléments de l'interface logicielle sur lesquels vous cliquez (par ex. option de menu, rubrique, champ d'option ou bouton).



2. Informations produit

Ce chapitre vous donne toutes les informations importantes pour l'acquisition et l'utilisation de votre produit Avira :

- voir chapitre : Prestations
- voir chapitre : Configuration requise
- voir chapitre : Attribution de licence et mise à niveau
- voir chapitre : Gestion des licences

Les produits Avira proposent des outils complets et flexibles pour protéger votre ordinateur de manière fiable contre les virus, logiciels malveillants, programmes indésirables et autres dangers.

- Attention :

Avertissement
La perte de données précieuses a souvent des conséquences dramatiques. Même le meilleur programme de protection antivirus ne peut pas vous protéger à cent pour cent de la perte de données. Effectuez régulièrement des copies de sauvegarde (backup) de vos données.

Remarque
Un programme qui protège des virus, logiciels malveillants, programmes indésirables et autres dangers n'est fiable et efficace que s'il est à jour. Assurez-vous de l'actualité de votre produit Avira grâce aux mises à jour automatiques. Configurez le programme en conséquence.

2.1 Prestations

Votre produit Avira dispose des fonctions suivantes :

- Control Center pour la surveillance, la gestion et la commande de l'intégralité du programme
- Configuration centrale intuitive en mode standard ou expert avec une aide contextuelle
- Scanner (On-Demand Scan) avec recherche configurable par profil de tous les types connus de virus et logiciels malveillants
- Intégration au contrôle du compte d'utilisateur (User Account Control) de Windows Vista pour pouvoir effectuer les tâches nécessitant des droits d'administrateur.
- Protection temps réel (On-Access Scan) pour la surveillance permanente de tous les accès aux données

- Composant ProActiv pour une surveillance permanente des actions de programme (uniquement pour systèmes 32 bits)
- Protection e-mail (scanner POP3, scanner IMAP et scanner SMTP) pour le contrôle permanent de vos e-mails à la recherche de virus et logiciels malveillants, notamment la vérification des pièces jointes
- Avira SearchFree Toolbar, une barre de recherche intégrée au navigateur Web vous permettant de faire des recherches rapides et agréables sur Internet. Elle contient également des widgets pour les principales fonctions d'Internet.
- Protection Web pour la vérification des données et fichiers transmis depuis Internet par protocole HTTP (surveillance des ports 80, 8080, 3128)
- Composant de contrôle parental pour un filtrage basé sur des rôles des sites Internet indésirables et pour la limitation de l'utilisation d'Internet
- Avira Free Android Security est une application visant à empêcher la perte et/ou le vol de votre appareil. Cette application propose des fonctions vous permettant de retrouver votre appareil mobile si vous l'avez égaré ou pire : s'il vous a été volé. En outre, elle peut bloquer des appels entrants ou SMS. Avira Free Android Security protège les téléphones mobiles et smartphones dotés d'un système d'exploitation Android.
- Composant de sauvegarde pour la création de sauvegardes de vos données (sauvegardes en miroir)
- Gestion de quarantaine intégrée pour l'isolation et le traitement des fichiers suspects
- Protection Rootkits pour identifier les logiciels malveillants installés de façon dissimulée sur le système de l'ordinateur (Rootkits) (non disponible sous Windows XP 64 bits)
- Accès direct aux informations détaillées sur les virus et logiciels malveillants trouvés via Internet
- Mise à jour simple et rapide du programme, des fichiers de définitions des virus (VDF) et du moteur de recherche grâce à la mise à jour de fichiers individuels et à la mise à jour incrémentielle VDF via un serveur Web basé sur Internet
- Gestion des licences simple et intuitive
- Planificateur intégré pour la définition de tâches uniques ou répétées comme les mises à jour et les contrôles
- Identification extrêmement efficace des virus et logiciels malveillants grâce à des technologies de recherche innovantes (moteur de recherche) comprenant des procédés de recherche heuristique
- Identification de tous les types d'archives courants, y compris des extensions d'archives imbriquées et des extensions intelligentes
- Grande performance grâce à la capacité de multithreading (scannage simultané de nombreux fichiers à vitesse élevée)
- FireWall pour protéger votre ordinateur des accès non autorisés depuis Internet ou un réseau ainsi que des accès non autorisés à Internet/à un réseau par des utilisateurs non autorisés

2.2 Configuration requise

La configuration requise suivante s'applique :

- Processeur Pentium et supérieur, au moins 1 GHz
- Système d'exploitation
  - Windows XP, dernier SP (32 ou 64 bits) ou
  - Windows 7, dernier SP (32 ou 64 bits)

> **Remarque**
> La certification Windows 8 pour Avira Internet Security est en cours.

- 150 Mo minimum d'espace mémoire disponible sur le disque dur (voire plus en cas d'utilisation de la fonction de quarantaine et pour la mémoire temporaire)
- 512 Mo minimum de mémoire vive sous Windows XP
- 1024 Mo minimum de mémoire vive sous Windows 7
- Pour l'installation du programme : droits d'administrateur
- Pour toutes les installations : Windows Internet Explorer 6.0 ou une version ultérieure
- Connexion Internet, le cas échéant (voir Installation)

Avira SearchFree Toolbar

- Système d'exploitation
  - Windows XP, dernier SP (32 ou 64 bits) ou
  - Windows 7, dernier SP (32 ou 64 bits)
- Navigateur Web
  - Windows Internet Explorer 6.0 ou une version ultérieure
  - Mozilla Firefox 3.0 ou une version ultérieure
  - Google Chrome 18.0 ou une version ultérieure

> **Remarque**
> Le cas échéant, désinstallez les barres de recherche déjà installées avant l'installation de l'Avira SearchFree Toolbar. Autrement, il sera impossible d'installer l'Avira SearchFree Toolbar.

Remarques pour les utilisateurs de Windows Vista

Sous Windows XP, de nombreux utilisateurs travaillent avec des droits d'administrateur. Ceci n'est toutefois pas souhaitable pour des raisons de sécurité, car les virus et programmes indésirables peuvent plus facilement s'immiscer dans l'ordinateur.

Par conséquent, avec Windows Vista, Microsoft instaure le « contrôle de compte d'utilisateur » (User Account Control). Cette fonction offre plus de protection aux utilisateurs connectés en tant qu'administrateur : un administrateur sous Windows Vista dispose par défaut uniquement des privilèges d'un utilisateur normal. Les actions pour lesquelles des droits d'administrateur sont nécessaires sont repérées par une icône par Windows Vista. En outre, l'utilisateur doit confirmer l'action souhaitée. Ce n'est qu'après avoir donné son accord que des privilèges plus importants sont octroyés et que le système d'exploitation exécute la tâche administrative en question.

Le produit Avira nécessite des droits d'administrateur pour quelques actions sous Windows Vista. Ces actions sont identifiées par le caractère suivant : . Si ce symbole apparaît en outre sur un bouton, des droits d'administrateur sont nécessaires pour cette action. Si votre compte utilisateur actuel ne dispose pas de droits d'administrateur, la boîte de dialogue de contrôle de compte d'utilisateur Windows Vista vous demande de saisir le mot de passe d'administrateur. Si vous ne disposez pas du mot de passe d'administrateur, vous ne pouvez pas exécuter cette action.

2.3 Attribution de licence et mise à niveau

2.3.1 Attribution de licence

Pour pouvoir utiliser votre produit Avira, il vous faut une licence. Vous acceptez ainsi les conditions de licence.

La licence est attribuée sous forme d'un code d'activation. Le code d'activation est un code alphanumérique que vous recevez à l'achat du produit Avira. Les données exactes de votre licence sont enregistrées par le biais du code d'activation, c'est-à-dire pour quels programmes et pour combien de temps la licence vous a été accordée.

Le code d'activation vous est transmis par e-mail si vous avez acheté votre produit Avira sur Internet ou se trouve sur l'emballage du produit.

Pour obtenir la licence de votre programme, entrez le code d'activation lors de l'activation du programme. L'activation du produit peut s'effectuer lors de l'installation. Vous pouvez toutefois aussi activer votre produit Avira après l'installation dans le gestionnaire de licences sous **Aide > Gestion des licences**.

2.3.2 Prolongation de la licence

Si votre licence arrive prochainement à expiration, Avira vous rappelle de la prolonger par l'intermédiaire d'un message-bannière. Il vous suffit alors de cliquer sur un lien pour accéder à la boutique en ligne d'Avira. Vous pouvez également prolonger la licence de votre produit Avira dans le gestionnaire de licences, sous **Aide > Gestion des licences**.

Si vous êtes enregistré sur le portail de gestion des licences d'Avira, vous pouvez aussi prolonger votre licence dans l'**Aperçu des licences** ou opter pour la prolongation automatique.

2.3.3 Mise à niveau

Dans le gestionnaire de licences, vous avez la possibilité de lancer la mise à jour d'un produit issue de la gamme de produits Avira Desktop : vous n'avez donc pas besoin de procéder à une désinstallation manuelle de l'ancien produit et à une installation manuelle du nouveau produit. En cas de mise à niveau à partir du gestionnaire de licences, indiquez le code d'activation du produit auquel vous voulez passer dans le champ de saisie du gestionnaire de licences. Une installation automatique du nouveau produit s'effectue alors.

Afin de garantir une fiabilité et une protection élevées pour votre ordinateur, Avira vous rappelle la mise à jour en attente de la nouvelle version. Cliquez sur **Mise à jour** dans l'élément pop up pour accéder à la page de mise à jour spécifique au produit. Vous pouvez effectuer une mise à jour de votre produit actuel ou acquérir un produit Avira avec davantage de fonctionnalités. La page d'aperçu des produits Avira vous montre le produit que vous utilisez actuellement et vous donne la possibilité de le comparer à d'autres produits Avira. Pour davantage d'informations, cliquez sur l'icône d'information à droite à côté du nom du produit. Si vous souhaitez conserver votre produit actuel, cliquez sur **Mise à jour** pour installer immédiatement la version la plus récente avec des fonctions optimisées. Pour acheter un produit plus complet, cliquez sur **Acheter** en bas de la colonne du produit concerné. Vous êtes dirigé vers la boutique en ligne Avira pour procéder à votre commande.

> **Remarque**
> Selon votre produit et votre système d'exploitation, vous devez éventuellement disposer des droits d'administrateur pour procéder à cette mise à jour. Connectez-vous en tant qu'administrateur avant d'effectuer une mise à jour.

2.3.4 Gestion des licences

La gestion des licences Avira Internet Security permet une installation très simple de la licence Avira Internet Security.

Gestion des licences Avira Internet Security



Vous pouvez effectuer une installation de la licence en sélectionnant le fichier de licence dans votre gestionnaire de fichiers ou l'e-mail d'activation en cliquant deux fois dessus et en suivant les instructions à l'écran.

> **Remarque**
> La gestion des licences Avira Internet Security copie la licence correspondante automatiquement dans le dossier de produit correspondant. Si une licence est déjà disponible, un message s'affiche demandant si le fichier de licence doit être remplacé. Dans ce cas, le fichier déjà existant est écrasé avec le fichier de licence actuel.



3. Installation et désinstallation

Dans ce chapitre, vous trouverez des informations sur l'installation et la désinstallation de votre produit Avira :

- voir chapitre : Avant l'installation : configuration requise, préparation de l'ordinateur à l'installation
- voir chapitre : Installation express : installation standard selon les paramètres par défaut
- voir chapitre : Installation personnalisée : installation configurable
- voir chapitre : Installation du produit test
- voir chapitre : Assistant de configuration
- voir chapitre : Installation modifiée
- voir chapitre : Modules d'installation
- voir chapitre : Désinstallation : procéder à la désinstallation

3.1 Types d'installation

Pendant l'installation, vous pouvez choisir un type de configuration dans l'assistant d'installation :

Express

- Les composants standard sont installés.
- Les fichiers de programme sont installés dans un répertoire par défaut sous *C:\Program Files*.
- Votre produit Avira est installé avec les paramètres par défaut. Vous n'avez pas la possibilité d'effectuer des préréglages dans l'assistant de configuration.

Personnalisé

- Vous avez la possibilité de sélectionner les divers composants du programme pour l'installation (voir chapitre Installation et désinstallation > Modules d'installation).
- Vous pouvez sélectionner un répertoire de destination pour les fichiers de programme à installer.
- Vous pouvez décider si un raccourci doit être créé sur votre Bureau et/ou un groupe de programmes doit être intégré dans le menu Démarrer.
- À l'aide de l'assistant de configuration, vous pouvez procéder à des paramétrages personnalisés de votre produit Avira et effectuer un rapide contrôle du système directement après l'installation.

3.2 Avant l'installation

Remarque
Avant de procéder à l'installation, vérifiez si votre ordinateur affiche la configuration requise. Si tel est le cas, vous pouvez installer le produit Avira.

Initialisation avant l'installation

✓ Fermez votre programme de messagerie électronique. Il est en outre recommandé de fermer toutes les applications ouvertes.
✓ Assurez-vous qu'aucune autre solution antivirus n'est installée. Les fonctions de protection automatiques des différentes solutions de sécurité peuvent entrer en conflit.

↪ Le produit Avira parcourt votre système pour détecter d'éventuels programmes incompatibles.

↪ Si le produit identifie des logiciels incompatibles, il génère la liste de ces programmes.

↪ Nous vous recommandons de désinstaller les programmes compromettant la sécurité de votre ordinateur.

▸ Dans cette liste, sélectionnez les programmes devant être supprimés automatiquement de votre ordinateur et cliquez sur **Suivant**.

▸ Certains programmes ne peuvent être supprimés que manuellement de votre ordinateur. Sélectionnez les programmes et cliquez sur **Suivant**.

↪ La désinstallation d'un ou plusieurs programmes nécessite le redémarrage de l'ordinateur. L'installation se poursuit après le redémarrage.

Attention
Votre ordinateur est sans protection jusqu'à la finalisation de la procédure d'installation du produit Avira.

Installation

Le programme d'installation fonctionne en mode de dialogue auto-explicatif. Lors des nombreuses étapes d'installation, un simple clic suffit pour continuer.

Les principaux boutons disposent des fonctions suivantes :

- **OK** : confirmer l'action.
- **Annuler** : abandonner l'action.
- **Suivant** : passer à l'étape suivante.
- **Retour** : revenir à l'étape précédente.

- Connectez-vous à Internet. La connexion Internet est nécessaire à l'exécution des étapes d'installation suivantes :
  - Téléchargement des fichiers de programme actuels et du moteur de recherche, ainsi que des fichiers de définitions des virus à jour par le biais du programme d'installation (en cas d'installation à partir d'Internet)
  - Activation du programme
  - Si nécessaire, exécution d'une mise à jour une fois l'installation terminée
- Ayez le code d'activation ou le fichier de licence à disposition lorsque vous souhaitez activer le programme.

> **Remarque**
> **Installation à partir d'Internet :**
> pour une installation à partir d'Internet, vous disposez d'un programme d'installation qui charge les fichiers de programme actuels à partir des serveurs Web Avira avant l'exécution de l'installation. Cette procédure garantit que votre produit Avira est installé avec un fichier de définitions des virus à jour.
>
> **Installation avec un pack d'installation :**
> le pack d'installation contient le programme d'installation et tous les fichiers de programme nécessaires. Cependant, lors d'une installation à l'aide d'un pack d'installation, il n'est pas possible de sélectionner la langue pour le produit Avira. Il est recommandé, à l'issue de l'installation, d'effectuer une mise à jour afin d'actualiser le fichier de définitions des virus.

> **Remarque**
> Pour activer le produit, le produit communique avec les serveurs d'Avira via le protocole HTTP et le port 80 (communication Web) ainsi que via le protocole de cryptage SSL et le port 443. Si vous utilisez un pare-feu, assurez-vous que celui-ci ne bloque pas les connexions nécessaires ni les données entrantes ou sortantes.

3.3 Installation express

Installation de votre produit Avira:

Lancez le programme d'installation par un double clic sur le fichier d'installation que vous avez téléchargé sur Internet ou insérez le CD du programme.

Installation à partir d'un téléchargement Internet

↳ L'écran **Bienvenue** s'affiche.

- Cliquez sur **Suivant** pour poursuivre l'installation.



↳ La boîte de dialogue **Sélection de la langue** s'affiche.

- Sélectionnez la langue dans laquelle vous souhaitez installer votre produit Avira et validez votre sélection de langue en cliquant sur **Suivant**.

  ↳ La boîte de dialogue **Téléchargement** s'affiche. Tous les fichiers nécessaires à l'installation sont téléchargés à partir des serveurs Web Avira. Une fois le téléchargement terminé, la fenêtre **Téléchargement** se referme.

Installation à l'aide d'un pack d'installation

↳ La fenêtre **Installation en cours de préparation** s'affiche.

↳ Le fichier d'installation est décompressé. La routine d'installation démarre.

↳ La boîte de dialogue **Sélection du type d'installation** s'affiche.

> **Remarque**
> L'installation express est activée par défaut. Tous les composants standard sont installés sans possibilité de configuration. Pour procéder à une installation personnalisée, consultez le chapitre Installation et désinstallation > Installation personnalisée.

- La case à cocher **Je souhaite améliorer ma protection en utilisant Avira Proactiv et Protection Cloud** (Configuration > Généralités > Protection avancée) est activée par défaut. Si vous ne souhaitez pas participer à la communauté Avira, décochez cette case.

  ↳ Si vous confirmez votre participation à la communauté Avira, Avira envoie les données sur les programmes suspects détectés à l'Avira Malware Research Center. Les données servent uniquement à une analyse en ligne avancée et au développement et à l'amélioration de la technologie de détection. Vous pouvez cliquer sur les liens **ProActiv** et **Protection Cloud** pour obtenir de plus amples détails sur l'analyse en ligne et dans le cloud améliorée.

- Confirmez que vous acceptez le **contrat de licence utilisateur final**. Pour lire l'intégralité du **contrat de licence utilisateur final**, cliquez sur le lien **CLUF**.

  ↳ L'**assistant de licence** s'ouvre et vous aide à activer votre produit.

  ↳ Ici, vous pouvez configurer un serveur proxy.

  - Le cas échéant, cliquez sur **Paramètres proxy** pour configurer le serveur proxy et confirmez vos paramètres avec **OK**.

  - Si vous avez déjà reçu un code d'activation, sélectionnez **Activer le produit** et saisissez ensuite votre code.

    -OU-

  - Si vous n'avez pas encore de code d'activation, cliquez sur le lien **Acheter un code d'activation**.

    ↳ Vous êtes redirigé vers le site Internet Avira.

Vous pouvez aussi cliquer sur le lien **Je possède déjà un fichier de licence valide**.

↳ La **boîte de dialogue Ouverture du fichier** s'affiche.

- Sélectionnez votre fichier de licence *.KEY* et cliquez sur **Ouvrir**.

↳ Le code d'activation est copié dans l'Assistant de licence.

- Si vous souhaitez tester le produit, reportez-vous au chapitre Installation de la version d'évaluation du produit.
- Cliquez sur **Suivant**.

↳ Une barre verte indique la progression de l'installation.

- Cliquez sur **Suivant**.

↳ La boîte de dialogue **Rejoindre les millions d'utilisateurs qui utilisent déjà Avira SearchFree** s'affiche.

- Si vous ne souhaitez pas installer Avira SearchFree Toolbar, décochez la case devant Avira SearchFree Toolbar et Avira SearchFree Updater **Contrat de licence d'utilisateur final**, puis celle qui définit **Avira SearchFree (search.avira.com)** comme page d'accueil de votre navigateur.

> **Remarque**
> Si nécessaire, désinstallez les barres de recherche déjà installées avant d'installer Avira SearchFree Toolbar. Sinon, vous ne pourrez pas installer Avira SearchFree Toolbar.

- Cliquez sur **Suivant**.

↳ Une barre verte indique la progression de l'installation de Avira SearchFree Toolbar.

↳ L'icône de barre d'état Avira est intégrée dans la barre des tâches.

↳ Le module **Updater** recherche les mises à jour éventuelles pour optimiser la protection de votre ordinateur.

↳ La fenêtre **Luke Filewalker** s'affiche pour lancer une première recherche directe du scanner, vous informe de l'état de la vérification et vous affiche les résultats.

- Si une fois le contrôle du système effectué, vous êtes invité à relancer l'ordinateur, procédez au redémarrage pour que votre système soit intégralement protégé.

Une fois l'installation réussie, il est recommandé de vérifier dans la zone **État** du Control Center si le programme de protection est à jour.

- Si votre produit Avira vous indique que votre ordinateur n'est pas totalement protégé, cliquez sur **Résoudre le problème**.

↳ La boîte de dialogue **Restaurer la protection** s'ouvre.

- Optimisez la sécurité de votre système en activant les options prescrites.

- Effectuez ensuite un contrôle intégral du système le cas échéant.

3.4 Installation personnalisée

Installation de votre produit Avira:

Lancez le programme d'installation par un double clic sur le fichier d'installation que vous avez téléchargé sur Internet ou insérez le CD du programme.

Installation à partir d'un téléchargement Internet

↳ L'écran **Bienvenue** s'affiche.

- Cliquez sur **Suivant** pour poursuivre l'installation.

  ↳ La boîte de dialogue **Sélection de la langue** s'affiche.

- Sélectionnez la langue dans laquelle vous souhaitez installer votre produit Avira et validez votre sélection de langue en cliquant sur **Suivant**.

  ↳ La boîte de dialogue **Téléchargement** s'affiche. Tous les fichiers nécessaires à l'installation sont téléchargés à partir des serveurs Web Avira. Une fois le téléchargement terminé, la fenêtre **Téléchargement** se referme.

Installation à l'aide d'un pack d'installation

↳ La fenêtre **Installation en cours de préparation** s'affiche.

↳ Le fichier d'installation est décompressé. La routine d'installation démarre.

↳ La boîte de dialogue **Sélection du type d'installation** s'affiche.

> **Remarque**
> L'installation express est activée par défaut. Tous les composants standard sont installés sans possibilité de configuration. Si vous souhaitez effectuer une Installation express, consultez le chapitre Installation et désinstallation > Installation express.

- Sélectionnez le type d'installation **Personnalisé**.
- L'option **Je souhaite améliorer ma protection avec Avira ProActiv et la protection Cloud** est sélectionnée par défaut. Si vous ne souhaitez pas rejoindre la communauté Avira, décochez cette case.

  ↳ Si vous confirmez votre participation à la communauté Avira, Avira envoie les données sur les programmes suspects détectés à l'Avira Malware Research Center. Les données servent uniquement à une analyse en ligne avancée et au développement et à l'amélioration de la technologie de détection. Vous pouvez cliquer sur les liens **ProActiv** et **Protection Cloud** pour obtenir de plus amples détails sur l'analyse en ligne et dans le cloud améliorée.

- Confirmez que vous acceptez le **contrat de licence utilisateur final**. Pour lire l'intégralité du **contrat de licence utilisateur final**, cliquez sur le lien correspondant.
- Cliquez sur **Suivant**.
  - ↳ La fenêtre **Sélectionner le répertoire d'installation** s'affiche.
  - ↳ Le répertoire *C:\Program Files\Avira\AntiVir Desktop* est paramétré par défaut
- Cliquez sur **Suivant** pour poursuivre l'installation.

  -OU-

  Avec **Parcourir**, choisissez un autre répertoire de destination et confirmez avec **Suivant**.
  - ↳ La boîte de dialogue **Installer les composants** s'affiche.
- Activez ou désactivez les composants souhaités et confirmez avec **Suivant**.
- Si vous avez sélectionné les composants **Protection Cloud**, mais souhaitez confirmer manuellement à chaque fois quels fichiers doivent être téléchargés pour la protection Cloud, activez l'option **Confirmer manuellement en cas d'envoi de fichiers suspects à Avira**.
- Cliquez sur **Suivant**.
- Dans la boîte de dialogue suivante, vous pouvez décider si un raccourci doit être créé sur votre Bureau et/ou un groupe de programmes dans le menu Démarrer.
- Cliquez sur **Suivant**.
  - ↳ L'**assistant de licence** s'ouvre.

Vous pouvez sélectionner les options suivantes pour activer le programme :

- Saisie d'un code d'activation.
  - ↳ En saisissant votre code d'activation, votre produit Avira et sa licence sont activés.
- Si vous n'avez pas encore de code d'activation, cliquez sur le lien **Acheter un code d'activation**.
  - ↳ Vous êtes redirigé vers le site Internet Avira.
- Sélection de l'option **Tester le produit**
  - ↳ Sélectionnez l'option **Tester le produit** pour générer une licence test permettant d'activer le programme lors du processus d'activation. Vous pouvez tester l'intégralité les fonctions du produit Avira pendant une période définie (voir Installation du produit test).

> **Remarque**
> L'option **Je possède déjà un fichier de licence valide** vous permet de lire un fichier de licence valide. Le fichier de licence est généré avec un code d'activation valide lors du processus d'activation du produit ; il est placé dans le

répertoire de votre produit Avira. Utilisez cette option si le produit est déjà activé et que vous souhaitez réinstaller votre produit Avira.

Remarque
Dans certaines versions de produits Avira, un code d'activation est déjà enregistré dans le produit. Il n'est donc pas nécessaire d'indiquer de code d'activation. Le cas échéant, le code d'activation enregistré est affichée dans l'assistant de licence.

Remarque
Une connexion aux serveurs Avira est établie pour l'activation du programme. Sous **Paramètres proxy**, vous pouvez configurer la connexion Internet via un serveur proxy.

- Sélectionnez un processus d'activation et confirmez en cliquant sur **Suivant**.
- Si vous disposez déjà d'un fichier de licence valide, passez directement à l'étape « Sélection de l'option *Je possède déjà un fichier de licence valide* ».

Activation de produit

↳ Une fenêtre de dialogue s'ouvre dans laquelle vous pouvez entrer vos données personnelles.

- Saisissez vos données et cliquez sur **Suivant**.

↳ Vos données sont transférées vers les serveurs Avira, puis vérifiées. Votre produit Avira est activé avec votre licence.

↳ Vos données de licence s'affichent dans la fenêtre de dialogue suivante.

- Cliquez sur **Suivant**.
- Ignorez l'étape suivante « Sélection de l'option *Je possède déjà un fichier de licence valide* ».

Sélection de l'option « Je possède déjà un fichier de licence valide »

↳ Une fenêtre de dialogue s'ouvre pour lire le fichier de licence.

- Sélectionnez le fichier de licence (sous la forme d'un fichier *.KEY*) avec vos données de licence pour le programme et cliquez sur **Ouvrir**.

↳ Vos données de licence s'affichent dans la fenêtre de dialogue suivante.

- Cliquez sur **Suivant**.

Une fois l'activation terminée ou le fichier de licence chargé

↳ La boîte de dialogue **Rejoindre les millions d'utilisateurs qui utilisent déjà Avira SearchFree** s'affiche.

- Si vous ne souhaitez pas installer Avira SearchFree Toolbar, désactivez les cases à cocher Avira SearchFree Toolbar et Avira SearchFree Updater dans le **contrat de licence utilisateur final** et la case qui définit **Avira SearchFree (search.avira.com)** comme page de démarrage de votre navigateur.

> **Remarque** Si nécessaire, désinstallez les barres de recherche déjà installées avant d'installer Avira SearchFree Toolbar. Sinon, vous ne pourrez pas installer Avira SearchFree Toolbar.

- Cliquez sur **Suivant**.

↳ L'**assistant d'installation** se ferme et l'assistant de configuration s'ouvre.

3.5 Installation du produit de test

Installation de votre produit Avira:

Lancez le programme d'installation par un double clic sur le fichier d'installation que vous avez téléchargé sur Internet ou insérez le CD du programme.

Installation à partir d'un téléchargement Internet

↳ L'écran **Bienvenue** s'affiche.

- Cliquez sur **Suivant** pour poursuivre l'installation.

↳ La boîte de dialogue **Sélection de la langue** s'affiche.

- Sélectionnez la langue dans laquelle vous souhaitez installer votre produit Avira et validez votre sélection de langue en cliquant sur **Suivant**.

↳ La boîte de dialogue **Téléchargement** s'affiche. Tous les fichiers nécessaires à l'installation sont téléchargés à partir des serveurs Web Avira. Une fois le téléchargement terminé, la fenêtre **Téléchargement** se referme.

Installation à l'aide d'un pack d'installation

↳ La fenêtre **Installation en cours de préparation** s'affiche.

↳ Le fichier d'installation est décompressé. La routine d'installation démarre.

↳ La boîte de dialogue **Sélection du type d'installation** s'affiche.

> **Remarque**
> L'**installation express** est activée par défaut. Tous les composants standard



sont installés sans possibilité de configuration. Si vous souhaitez effectuer une Installation personnalisée, consultez le chapitre Installation et désinstallation > Installation personnalisée.

- La case à cocher **Je souhaite améliorer ma protection en utilisant Avira Proactiv et Protection Cloud** (Configuration > Généralités > Protection avancée) est activée par défaut. Si vous ne souhaitez pas rejoindre la communauté Avira, décochez cette case.
  - ↳ Si vous confirmez votre participation à la communauté Avira, Avira envoie les données sur les programmes suspects détectés à l'Avira Malware Research Center. Les données servent uniquement à une analyse en ligne avancée et au développement et à l'amélioration de la technologie de détection. Vous pouvez cliquer sur les liens **ProActiv** et **Protection Cloud** pour obtenir de plus amples détails sur l'analyse en ligne et dans le cloud améliorée.
- Confirmez que vous acceptez le **contrat de licence utilisateur final**. Pour lire l'intégralité du **contrat de licence utilisateur final**, cliquez sur le lien correspondant.
- Cliquez sur **Suivant**.
  - ↳ L'**assistant de licence** s'ouvre et vous aide à activer votre produit.
  - ↳ Ici, vous pouvez configurer un **serveur proxy**.
- Cliquez sur **Paramètres du proxy** pour effectuer la configuration et confirmez vos paramètres avec **OK**.
- Sélectionnez l'option **Produit de test** dans l'assistant de licence et cliquez sur **Suivant**.
- Renseignez les champs obligatoires sous **Enregistrement**. Choisissez si vous vous abonnez ou non à la **Lettre d'information Avira** et cliquez sur **Suivant**.
  - ↳ Une barre verte indique la progression de l'installation.
  - ↳ La boîte de dialogue **Rejoignez les millions d'utilisateurs qui utilisent déjà Avira SearchFree Toolbar** s'affiche.
- Si vous ne souhaitez pas installer Avira SearchFree Toolbar, désactivez les cases à cocher Avira SearchFree Toolbar et Avira SearchFree Updater dans le **contrat de licence utilisateur final** et la case qui définit **Avira SearchFree (search.avira.com)** comme page de démarrage de votre navigateur.

Remarque
Si nécessaire, désinstallez les barres de recherche déjà installées avant d'installer Avira SearchFree Toolbar. Sinon, vous ne pourrez pas installer Avira SearchFree Toolbar.

- Cliquez sur **Suivant**.
- Vous serez invité à redémarrer votre système pour activer votre produit Avira. Cliquez sur **Oui** pour redémarrer immédiatement votre ordinateur.



↳ L'icône de barre d'état Avira est intégrée dans la barre des tâches.

↳ Votre licence d'évaluation est valable pendant 31 jours.

3.6 Assistant de configuration

En cas d'installation personnalisée, l'assistant de configuration s'ouvre à la fin de la procédure. L'assistant de configuration vous permet de définir des paramètres importants de votre produit Avira.

- Dans la fenêtre de bienvenue de l'assistant de configuration, cliquez sur **Suivant** pour commencer la configuration du programme.

  ↳ Dans la fenêtre de dialogue **Configurer AHeAD**, vous pouvez choisir un degré d'identification pour la technologie AHeAD. Le degré d'identification choisi est repris pour le paramétrage de la technologie AHeAD du scanner (recherche directe) et de la protection temps réel (recherche en temps réel).

- Choisissez un degré d'identification et poursuivez la configuration avec **Suivant**.

  ↳ Dans la boîte de dialogue suivante **Sélectionner des catégories de dangers étendues**, vous pouvez adapter les fonctions de protection de votre produit Avira avec la sélection des catégories de dangers.

- Le cas échéant, sélectionnez des catégories de dangers supplémentaires et poursuivez la configuration en cliquant sur **Suivant**.

  ↳ Si vous avez sélectionné le module d'installation Avira FireWall pour l'installation , la boîte de dialogue **Règles par défaut pour l'accès au réseau et l'utilisation des ressources réseau** s'affiche à l'écran. Vous pouvez déterminer si Avira FireWall doit autoriser les accès externes aux ressources autorisées ainsi que les accès réseau d'applications d'entreprises fiables.

- Activez les options souhaitées et poursuivez la configuration en cliquant sur **Suivant**.

  ↳ Si vous avez choisi le module d'installation Protection temps réel Avira, la boîte de dialogue **Mode de démarrage de la protection temps réel** s'affiche. Vous pouvez définir le moment du démarrage de la protection temps réel. La protection temps réel démarre dans le mode de démarrage indiqué, à chaque redémarrage de l'ordinateur.

Remarque
Le mode de démarrage indiqué de la protection temps réel est consigné dans le Registre et ne peut pas être modifié par la configuration.

Remarque
Au démarrage de l'ordinateur, la sélection du mode de démarrage par défaut pour la protection temps réel (démarrage normal) et une connexion rapide au compte utilisateur évite, notamment, le scannage des programmes démarrant

automatiquement, dans la mesure où ceux-ci sont démarrés avant le chargement complet de la protection temps réel.

- Activez l'option souhaitée et poursuivez la configuration avec **Suivant**.
  - ↳ Si vous avez choisi le module d'installation Protection Web Avira, la boîte de dialogue **Navigation sécuriséeNavigation sécurisée** s'affiche. Vous avez la possibilité d'attribuer à l'utilisateur de l'ordinateur différents rôles pour l'utilisation d'Internet (enfant, adolescent, adulte). Vous pouvez également désactiver l'option Navigation sécurisée.
- Procédez aux réglages souhaités pour la Navigation sécurisée et poursuivez la configuration avec **Suivant**.
  - ↳ La boîte de dialogue suivante **Attribuer un mot de passe** vous permet de protéger l'accès à la configuration par mot de passe. Cette protection est particulièrement recommandée lorsque la Navigation sécurisée est activée.
  - ↳ La boîte de dialogue suivante **Contrôle du système** permet d'activer ou de désactiver l'exécution d'un contrôle rapide du système. Ce rapide contrôle du système est exécuté une fois la configuration terminée et avant le redémarrage de l'ordinateur. Il parcourt les programmes lancés et les fichiers système les plus importants, à la recherche de virus et de logiciels malveillants.
- Activez ou désactivez l'option **Contrôle rapide du système** et poursuivez la configuration avec **Suivant**.
  - ↳ La boîte de dialogue suivante vous permet de finaliser la configuration en cliquant sur **Terminer**.
  - ↳ Les réglages indiqués et sélectionnés sont validés.
  - ↳ Si vous avez activé l'option **Contrôle rapide du système**, la fenêtre **Luke Filewalker** s'ouvre. Le scanner effectue un contrôle rapide du système.
  - ↳ Si une fois le contrôle du système effectué, vous êtes invité à relancer l'ordinateur, procédez au redémarrage pour que votre système soit intégralement protégé.

Une fois l'installation réussie, il est recommandé de vérifier dans la zone **État** du Control Center si le programme de protection est à jour.

- Si votre produit Avira vous indique que votre ordinateur n'est pas totalement protégé, cliquez sur **Résoudre le problème**.
  - ↳ La boîte de dialogue **Restaurer la protection** s'ouvre.
- Optimisez la sécurité de votre système en activant les options prescrites.
- Effectuez ensuite un contrôle intégral du système le cas échéant.



3.7 Installation modifiée

Vous avez la possibilité d'ajouter ou de supprimer certains composants de programme de l'installation actuelle du produit Avira (voir chapitre Installation et désinstallation > Modules d'installation)

Si vous souhaitez ajouter ou supprimer des composants de programme de l'installation actuelle, vous pouvez utiliser l'option **Programmes** dans le **Panneau de configuration Windows** pour **Modifier/Supprimer** des programmes.

Sélectionnez votre produit Avira et cliquez sur **Modifier**. Dans la boîte de dialogue *Bienvenue* du programme, sélectionnez l'option **Modifier le programme**. Le système vous guide pas à pas pour procéder à l'installation modifiée.

3.8 Modules d'installation

Lors d'une installation personnalisée ou modifiée, les modules suivants peuvent être sélectionnés pour l'installation, ou ajoutés ou supprimés :

- **Avira Internet Security**
  Ce module contient tous les composants nécessaires à l'installation correcte de votre produit Avira.
- **Protection temps réel**
  La protection temps réel Avira est exécutée en arrière-plan. Il surveille et répare si possible les fichiers lors d'opérations comme l'ouverture, l'écriture et la copie en temps réel (On-Access = à l'accès). Si un utilisateur effectue une opération sur le fichier (charger, exécuter ou copier le fichier), le produit Avira parcourt automatiquement le fichier. Lors de l'opération Renommer, aucune recherche de la protection temps réel Avira n'est effectuée.
- **Protection e-mail**
  La protection e-mail sert d'interface entre votre ordinateur et le serveur e-mail à partir duquel votre programme de messagerie (client de messagerie) télécharge les e-mails. La protection e-mail sert de proxy entre le programme de messagerie et le serveur e-mail. Tous les e-mails entrants sont transférés via ce proxy, la présence de virus et de programmes indésirables est recherchée, puis ils sont transmis à votre programme de messagerie. Selon la configuration, le programme traite les e-mails automatiquement ou demande à l'utilisateur quoi faire. En outre, la protection e-mail peut vous protéger efficacement contre les spams.
- **Avira FireWall**
  L'Avira FireWall contrôle les voies de communication en provenance et à destination de votre ordinateur. Il autorise ou refuse la communication sur la base des consignes de sécurité.
- **Protection Rootkits**
  La Protection Rootkits Avira contrôle si un logiciel qui ne peut être détecté par les méthodes habituelles après infiltration dans votre système s'est déjà installé sur votre ordinateur.

- **ProActiv**
  Le composant ProActiv surveille les actions des applications et signale les comportements suspects de celles-ci. Grâce à cette détection basée sur le comportement, vous pouvez vous protéger contre des logiciels malveillants inconnus. Le composant ProActiv est intégré à la protection temps réel Avira.
- **Protection Cloud**
  Les composants de la protection Cloud constituent un module destiné à la détection en ligne dynamique de logiciels malveillants encore inconnus.
- **Sauvegarde**
  Le composant Sauvegarde vous permet de créer manuellement et de manière automatisée des sauvegardes en miroir de vos données.
- **Protection Web**
  En navigant sur Internet, via votre navigateur Web, vous sollicitez des données d'un serveur Web. Les données transmises par le serveur Web (fichiers HTML, script et images, fichiers flash, flux vidéo et musique, etc.) arrivent normalement de la mémoire cache du navigateur directement pour être exécutées dans le navigateur Web, ce qui exclut un contrôle par une recherche en temps réel comme la protection temps réel Avira le propose. De cette manière, des virus et programmes indésirables peuvent pénétrer dans votre système. La protection Web est un proxy HTTP qui surveille les ports (80, 8080, 3128) servant à la transmission des données et contrôle l'absence de virus et de programmes indésirables dans les données transférées. Selon la configuration, le programme traite les fichiers concernés automatiquement ou demande à l'utilisateur quelle action entreprendre.
- **Extension d'environnement**
  L'extension d'environnement génère dans le menu contextuel de l'explorateur Windows (bouton droit de la souris) l'entrée *Contrôler les fichiers sélectionnés avec Avira*. Avec cette entrée, vous pouvez scanner directement certains fichiers ou répertoires.

3.9 Désinstallation

Pour supprimer votre produit Avira de votre ordinateur, vous pouvez utiliser l'option **Programmes** pour **Modifier ou supprimer** des programmes dans le Panneau de configuration Windows.

Pour désinstaller votre produit Avira, procédez de la façon suivante (sur l'exemple de Windows 7) :

- Ouvrez le **Panneau de configuration** via le menu **Démarrer** de Windows.
- Double-cliquez sur **Programmes et fonctionnalités**.
- Sélectionnez votre produit Avira dans la liste et cliquez sur **Désinstaller**.
  - ↪ Le système vous demande si vous souhaitez réellement supprimer le programme.
- Confirmez avec **Oui**.

↳ Le système vous demande si le pare-feu Windows doit être réactivé (car l'Avira FireWall va être désactivé).

- Confirmez avec **Oui**.

↳ Tous les composants du programme sont supprimés.

- Cliquez sur **Terminer** pour terminer la désinstallation.

↳ Une fenêtre de dialogue peut s'afficher vous conseillant de redémarrer l'ordinateur.

- Confirmez avec **Oui**.

↳ Le produit Avira est désinstallé, votre ordinateur est redémarré si besoin est, ce faisant, tous les répertoires, tous les fichiers et toutes les entrées de Registre du programme sont supprimés.

Remarque
L'Avira SearchFree Toolbar n'est pas intégrée dans la désinstallation du programme, mais doit être désinstallée de façon individuelle en reproduisant la procédure ci-dessus. Pour ce faire, l'Avira SearchFree Toolbar doit être activée dans le gestionnaire de modules complémentaires. Une fois la désinstallation achevée, la barre de recherche n'est plus intégrée dans votre navigateur.

4. Aperçu d'Avira Internet Security

Dans ce chapitre, vous obtenez une vue d'ensemble des fonctionnalités et de l'utilisation de votre produit Avira.

- voir chapitre Interface et utilisation
- voir chapitre Avira SearchFree Toolbar
- voir chapitre Comment procéder

4.1 Interface et utilisation

L'utilisation de votre produit Avira se fait via trois éléments d'interface du programme :

- Control Center : surveillance et gestion du produit Avira
- Configuration : configuration du produit Avira
- Icône de la barre d'état dans la zone de notification de la barre des tâches : ouverture du Control Center et d'autres fonctions

4.1.1 Control Center

Le Control Center sert à vérifier l'état de protection de votre ordinateur, à gérer et à utiliser les composants de protection et les fonctions de votre produit Avira.

La fenêtre du Control Center se divise en trois zones : la **barre de menu**, la **zone de navigation** et la fenêtre de détail **État** :

- **Barre de menu :** dans les menus du Control Center, vous pouvez accéder aux fonctions générales du programme et à des informations sur le produit.
- **Zone de navigation :** la zone de navigation vous permet de passer d'une rubrique à l'autre du Control Center. Les différentes rubriques contiennent des informations et fonctions des composants du programme et sont classées dans la barre de navigation selon les champs d'action. Exemple : champ d'action *SÉCURITÉ PC* - rubrique **Protection temps réel**.
- **État :** l'écran de démarrage **État** vous indique immédiatement si votre ordinateur est suffisamment protégé, ainsi que les modules actifs, la date de la dernière sauvegarde et le dernier contrôle du système. La fenêtre **État** comprend tous les boutons de fonctions ou d'actions, comme l'activation ou la désactivation de la **protection temps réel**.

Démarrage et arrêt du Control Center

Vous disposez des options suivantes pour démarrer le Control Center :

- Cliquez deux fois sur l'icône du programme sur le Bureau

- Via l'entrée de programme dans le menu **Démarrer > Programmes**.
- Via l'icône de la barre d'état de votre produit Avira.

Vous quittez le Control Center via la commande de menu **Quitter** dans le menu **Fichier**, avec la commande clavier **Alt+F4** ou en cliquant sur la croix de fermeture dans le Control Center.

Utilisation du Control Center

Voici comment naviguer dans le Control Center :

▸ Cliquez dans la barre de navigation sur un champ d'action sous une rubrique.

↳ Le champ d'action apparaît avec les autres options de fonctions et de configuration dans la fenêtre de détail.

▸ Cliquez, le cas échéant, sur un autre champ pour les afficher dans la fenêtre de détail.

> **Remarque**
> La touche [**Alt**] permet d'activer la navigation au clavier dans la barre de menus. La touche **Entrée** vous permet d'activer la rubrique actuellement sélectionnée. Pour ouvrir et fermer des menus du Control Center, ou parcourir ceux-ci, vous pouvez également utiliser des raccourcis clavier : touche [**Alt**] + lettre soulignée du menu ou de la commande de menu. Maintenez la touche [**Alt**] enfoncée quand vous souhaitez accéder à une commande de menu ou à un sous-menu à partir du menu.

Voici comment traiter les données ou objets affichés dans la fenêtre de détail :

▸ Sélectionnez les données ou objets que vous souhaitez traiter.

Pour sélectionner plusieurs éléments, maintenez la touche **Ctrl** ou **Maj** (sélection d'éléments situés les uns sous les autres) enfoncée pendant la sélection des éléments.

▸ Cliquez sur le bouton souhaité dans la barre supérieure de la fenêtre de détail pour traiter l'objet.

Aperçu du Control Center

- **État** : l'écran de démarrage **État** présente toutes les rubriques vous permettant de surveiller les fonctionnalités du programme (voir État).
  - La fenêtre **État** vous permet de voir d'un seul coup d'œil quels modules sont actifs et fournit des informations sur la dernière mise à jour effectuée.
- *SÉCURITÉ PC* : vous trouverez ici les composants vous permettant de contrôler l'absence de virus et de logiciels malveillants dans les fichiers de votre ordinateur.
  - La rubrique **Scanner** vous permet de configurer et de démarrer simplement la recherche directe (voir Scanner). Les profils prédéfinis permettent d'effectuer une

recherche avec des options standard adaptées. À l'aide de la sélection manuelle (qui est enregistrée) ou en créant des profils personnalisés, vous pouvez également adapter la recherche de virus et de programmes indésirables à vos besoins personnels.

  - La rubrique Protection temps réel vous fournit des informations sur les fichiers contrôlés, ainsi que d'autres données statistiques, pouvant être réinitialisées à tout moment, et vous permet d'accéder au fichier rapport. Des informations plus détaillées sur le dernier virus ou programme indésirable trouvé sont disponibles en un clic.
  - La rubrique **Sauvegarde** vous permet d'effectuer simplement et rapidement des sauvegardes de vos données et de créer des tâches de sauvegarde (voir Sauvegarde).

- *SÉCURITÉ INTERNET* : vous trouverez ici les composants vous permettant de protéger votre ordinateur contre les virus et logiciels malveillants provenant d'Internet et les accès réseau indésirables.
  - La rubrique **FireWall** vous permet de configurer les paramètres de base de l'Avira FireWall . En outre, les débits actuels et toutes les applications actives utilisant une connexion réseau s'affichent (voir FireWall).
  - La rubrique Protection Web vous fournit des informations sur les URL contrôlées et les virus trouvés, ainsi que d'autres données statistiques qu'il est possible de réinitialiser à tout moment, et vous permet d'afficher le fichier rapport. Des informations plus détaillées sur le dernier virus ou programme indésirable trouvé sont disponibles en un clic.
  - La rubrique **Protection e-mail** vous indique les e-mails contrôlés par ce service, leurs propriétés ainsi que d'autres données statistiques. En outre, vous avez la possibilité de personnaliser le filtre AntiSpam et d'exclure à l'avenir des adresses e-mail de la vérification anti-logiciels malveillants et anti-spam. Les e-mails peuvent également être supprimés de la mémoire tampon de la protection e-mail. (voir Protection e-mail).
- *CONTRÔLE PARENTAL* : vous trouverez ici des outils vous permettant de veiller à ce que vos enfants utilisent le Web en toute sécurité.
  - Navigation sécurisée : des rôles peuvent être attribués aux utilisateurs de l'ordinateur. Un rôle utilisateur peut être configuré et comprend un ensemble de règles avec les critères suivants : URL autorisées ou interdites (adresses Internet), catégories de contenu interdites, durée d'utilisation d'Internet et, le cas échéant, périodes d'utilisation autorisées par jour
- *PROTECTION MOBILE* : la catégorie Avira Free Android Security vous permet d'accéder en ligne à vos appareils Android.
  - Avira Free Android Security vous permet de gérer tous vos appareils dotés d'un système d'exploitation Android.
- *ADMINISTRATION* : vous trouverez ici des outils vous permettant d'isoler et de gérer les fichiers suspects ou infectés par des virus ainsi que de planifier des tâches récurrentes.



- Sous la rubrique **Quarantaine** se trouve le gestionnaire de quarantaines. Il s'agit de l'emplacement central pour les fichiers déjà en quarantaine ou pour les fichiers suspects que vous souhaitez mettre en quarantaine (voir Quarantaine). En outre, vous avez la possibilité d'envoyer un fichier par e-mail à l'Avira Malware Research Center.
- La rubrique **Planificateur** vous permet de créer des tâches de contrôle et de mise à jour programmées ainsi que des tâches de sauvegarde et d'adapter ou de supprimer les tâches existantes (voir Planificateur).
- La rubrique **Rapports** vous permet de visualiser les résultats des actions effectuées (voir Rapports).
- La rubrique **Événements** vous permet de vous informer sur les événements générés par les modules du programme (voir Événements).

4.1.2 Mode jeu

Si vous exécutez sur votre ordinateur des applications qui nécessitent le mode plein écran, vous pouvez bloquer de manière ciblée les notifications de Bureau et avertissements, tels que les fenêtres contextuelles et les alertes concernant les produits, en activant le mode jeu. En mode jeu, toutes les règles d'applications et d'adaptation définies dans la configuration de l'Avira FireWall sont utilisées sans que vous soyez averti des événements survenant sur le réseau.

Un clic sur le bouton **Activé/Désactivé** vous permet d'activer le mode jeu ou de définir le mode automatique. Par défaut, le mode jeu est configuré avec l'option **automatique** et est représenté en vert. Ce paramètre par défaut permet à votre produit Avira de basculer automatiquement dans le mode jeu lorsqu'une application est affichée en plein écran.

- Cliquez sur le bouton à gauche à côté de **Désactivé**, pour activer le mode jeu.
  - ↳ Le mode jeu est activé et le bouton s'affiche en jaune.

> **Remarque**
> Nous vous conseillons de ne modifier que temporairement le statut prédéfini **Désactivé** avec sa détection automatique d'applications en plein écran, car, en mode jeu, les notifications de Bureau et les avertissements ne s'affichent pas pour vous signaler les accès au réseau et les dangers éventuels.

4.1.3 Configuration

Dans la configuration, vous pouvez définir les paramètres de votre produit Avira. Après l'installation, votre produit Avira est configuré avec les paramètres par défaut qui garantissent une protection optimale de votre ordinateur. Toutefois, votre ordinateur ou vos exigences envers votre produit Avira peuvent présenter des particularités nécessitant l'ajustement de la configuration des composants de protection du programme.

La configuration se présente sous la forme d'une fenêtre de dialogue : les boutons **OK** ou **Appliquer** vous permettent d'enregistrer les paramètres définis dans la configuration, **Annuler** vous permet d'annuler vos paramètres et le bouton **Valeurs par défaut** vous permet de réinitialiser les paramètres de la configuration aux valeurs par défaut. Dans la barre de navigation à gauche, vous pouvez choisir les diverses rubriques de configuration.

Accès à la configuration

Vous avez plusieurs possibilités pour accéder à la configuration :

- Via le Panneau de configuration de Windows.
- Via le Centre de sécurité Windows - à partir de Windows XP Service Pack 2.
- Via l'icône de la barre d'état de votre programme Avira.
- Dans le Control Center via la rubrique Extras > Configuration.
- Dans le Control Center via le bouton Configuration.

Remarque
Si vous accédez à la configuration via le bouton **Configuration** du Control Center, vous arrivez dans le répertoire de configuration de la rubrique active dans le Control Center. Pour sélectionner les différents répertoires de

configuration, le **mode expert** de la configuration doit être activé. Dans ce cas, une boîte de dialogue s'affiche vous invitant à activer le **mode expert**.

Gestion de la configuration

Vous naviguez dans la fenêtre de configuration comme dans l'explorateur Windows :

- Cliquez sur une entrée de l'arborescence pour afficher cette rubrique de configuration dans la fenêtre de détail.
- Cliquez sur le signe plus devant une entrée pour agrandir la rubrique de configuration et afficher les sous-rubriques de la configuration dans l'arborescence.
- Pour masquer les sous-rubriques de la configuration, cliquez sur le signe moins devant la rubrique de configuration agrandie.

> **Remarque**
> Pour activer ou désactiver des options dans la configuration et appuyer sur des boutons, vous pouvez également utiliser les raccourcis clavier : touche [**Alt**] + lettre soulignée dans le nom de l'option ou de la désignation du bouton.

> **Remarque**
> Seul le mode expert permet d'afficher la totalité des rubriques de configuration. Activez le **mode expert** pour voir toutes les rubriques de configuration. Le **mode expert** peut être doté d'un mot de passe pour son activation.

Si vous souhaitez valider vos paramètres dans la configuration :

- Cliquez sur le bouton **OK**.

  ↳ La fenêtre de configuration se ferme et les paramètres sont validés.

  - OU -

  Cliquez sur le bouton **Valider**.

  ↳ Les paramètres définis sont validés. La fenêtre de configuration reste ouverte.

Si vous souhaitez quitter la configuration sans valider vos paramètres :

- Cliquez sur le bouton **Annuler**.

  ↳ La fenêtre de configuration se ferme et les paramètres sont rejetés.

Si vous souhaitez réinitialiser tous les paramètres de la configuration aux valeurs par défaut :

- Cliquez sur **Valeurs par défaut**.

↳ Tous les paramètres de la configuration sont réinitialisés aux valeurs par défaut. Toutes les modifications et vos saisies sont perdues en cas de restauration des valeurs par défaut.

Aperçu des options de configuration

Vous disposez des options de configuration suivantes :

- **Scanner** : configuration de la recherche directe
  - Options de recherche
  - Action si résultat positif
  - Options pour la recherche dans les archives
  - Exceptions de la recherche directe
  - Heuristique de la recherche directe
  - Réglage de la fonction de rapport
- **Protection temps réel** : configuration de la recherche en temps réel
  - Options de recherche
  - Action si résultat positif
  - Autres actions
  - Exceptions de la recherche en temps réel
  - Heuristique de la recherche en temps réel
  - Réglage de la fonction de rapport
- **Sauvegarde** :
  - Réglage du composant de sauvegarde (sauvegarde incrémentielle, recherche de virus lors de la sauvegarde)
  - Exceptions : réglage des fichiers à sauvegarder
  - Réglage de la fonction de rapport
- **Mise à jour** : configurations des paramètres de mise à jour
- **FireWall** : configuration du FireWall
  - Réglage des règles d'adaptation
  - Réglage personnalisé des règles d'applications
  - Liste des fournisseurs dignes de confiance (exceptions lors de l'accès réseau par des applications)
  - Paramètres avancés : dépassement de délai des règles, interrompre le pare-feu Windows, notifications
  - Paramètres popup (messages d'avertissement lors de l'accès réseau par des applications)
- **Protection Web** : configuration de la protection Web
  - Options de recherche, activation et désactivation de la protection Web
  - Action si résultat positif



  - Accès bloqués : types de fichiers et types MIME indésirables, filtre Web pour les URL connues indésirables (logiciels malveillants, hameçonnage, etc.)
  - Exceptions de recherche de la protection Web : URL, types de fichiers, types MIME
  - Heuristique de la protection Web
  - Réglage de la fonction de rapport
- **Protection e-mail** : configuration de la protection e-mail
  - Options de recherche : activation de la surveillance des comptes POP3, des comptes IMAP, des e-mails sortants (SMTP)
  - Action si résultat positif
  - Autres actions
  - Heuristique de la recherche de la protection e-mail
  - Fonction AntiBot : serveurs SMTP autorisés, expéditeurs d'e-mails autorisés
  - Exceptions de la recherche de la protection e-mail
  - Configuration de la mémoire tampon, vider la mémoire tampon
  - Configuration de la banque de données d'apprentissage AntiSpam, vider la banque de données d'apprentissage
  - Configuration d'un bas de page dans les e-mails envoyés
  - Réglage de la fonction de rapport
- **Contrôle parental** :
  - Navigation sécurisée : fonction de contrôle parental avec filtre basé sur des rôles et limitation de temps d'utilisation d'Internet basée sur des rôles
- **Généralités** :
  - Catégories étendues de dangers pour la recherche directe et en temps réel
  - Protection étendue : activer ProActiv et la protection Cloud
  - Filtre des applications : bloquer ou autoriser des applications
  - Protection par mot de passe pour l'accès au Control Center et à la configuration
  - Sécurité : bloquer les fonctions Autorun, verrouiller les fichiers hôtes Windows, protection du produit
  - WMI : activer la prise en charge WMI
  - Configuration de la consignation des événements
  - Configuration des fonctions de rapport
  - Réglage des répertoires utilisés
  - Configuration des avertissements sonores en cas de détection de logiciel malveillant

4.1.4 Icône de la barre d'état

Après l'installation, l'icône de barre d'état de votre produit Avira s'affiche dans la zone de notification de la barre des tâches :

Icône	Description
	La protection temps réel Avira est activée et le FireWall est activé
	La protection temps réel Avira est désactivée ou le FireWall est désactivé

L'icône dans la barre des tâches affiche l'état de la Protection temps réel et du Firewall .

Les fonctions centrales de votre produit Avira sont rapidement accessibles via le menu contextuel de l'icône de la barre d'état.

- Pour accéder au menu contextuel, cliquez avec le bouton droit de la souris sur l'icône de la barre d'état.

Entrées dans le menu contextuel

- **Activer la protection temps réel** : active ou désactive la protection temps réel Avira.
- **Activer la protection e-mail** : active ou désactive la protection e-mail Avira.
- **Activer la protection Web** : active ou désactive la protection Web Avira.
- **FireWall** :
  - **Activer le FireWall** : active ou désactive l'Avira FireWall
  - **Bloquer tous les transferts** : activé : bloque tout transfert de données à l'exception des transferts vers le système de l'ordinateur en question (Local Host / IP 127.0.0.1).
- **Démarrer Avira Internet Security** : ouvre le Control Center.
- **Configurer Avira Internet Security : ouvre la configuration.**
- **Mes messages : ouvre un message-bannière avec les derniers messages concernant votre produit Avira.**
- **Mes paramètres de communication : ouvre le centre d'abonnement pour les notifications produits**
- **Démarrer mise à jour : démarre une mise à jour.**
- **Aide : ouvre l'aide en ligne.**
- **À propos de Avira Internet Security : ouvre une boîte de dialogue avec des informations sur votre produit Avira : informations sur le produit, la version, la licence.**
- **Avira sur Internet : ouvre le portail Web Avira sur Internet. Un accès Internet est nécessaire.**



4.2 Avira SearchFree Toolbar

L'Avira SearchFree Toolbar comprend deux principaux composants : Avira SearchFree et la barre d'outils.

La nouvelle Avira SearchFree Toolbar s'installe sous la forme de module complémentaire. Lorsque vous accédez la première fois au navigateur (Internet Explorer ou Firefox), un message vous demande si vous acceptez que le programme de l'Avira SearchFree Toolbar modifie votre navigateur. Vous devez accepter afin de garantir le succès de l'installation de l'Avira SearchFree Toolbar.

Avira SearchFree est le nouveau moteur de recherche d'Avira et contient un logo Avira sur lequel vous pouvez cliquer pour être redirigé vers le site Web d'Avira, ainsi que des canaux Web et d'images. Il permet aux utilisateurs d'Avira d'effectuer une recherche complète et plus sûre.

La barre d'outils est intégrée à votre navigateur Web et comprend un champ de recherche, un logo Avira redirigeant vers le site Web d'Avira, deux affichages d'état, trois widgets et le menu **Options**.

- Barre de recherche
  Utilisez la barre de recherche pour naviguer sur Internet rapidement et gratuitement à l'aide du moteur de recherche Avira SearchFree.
- Affichage d'état
  Les affichages d'état décrivent l'état de la protection Web et le statut de mise à jour actuel de votre produit Avira, et vous permettent d'identifier les actions à entreprendre pour protéger votre PC.
- Widgets
  Avira vous permet d'accéder directement aux fonctions importantes sur Internet, par exemple vos messages Facebook ou votre messagerie. Vous pouvez également définir la protection de votre système grâce au widget Protection Web (uniquement sur Firefox et Internet Explorer).
- Options
  Le menu Options vous permet d'accéder aux options de Toolbar, d'effacer l'historique de recherche, de consulter l'aide et les informations concernant la barre d'outils et de désinstaller l'Avira SearchFree Toolbar directement à partir du navigateur Web (Firefox et Internet Explorer uniquement).

4.2.1 Utilisation

Barre de recherche

La barre de recherche vous permet de rechercher un ou plusieurs termes sur Internet.

Saisissez à cet effet le terme dans le champ de recherche et cliquez sur la touche **Entrée** ou cliquez sur **Recherche**. L'outil de recherche Avira SearchFree parcourt Internet pour vous et affiche tous les résultats dans la fenêtre du navigateur.

Vous pouvez configurer Avira SearchFree à votre guise dans **Options** sur Internet Explorer, Firefox et Chrome.

Affichage d'état

Protection Web

Pour déterminer l'état de sécurité de votre ordinateur, vous pouvez utiliser les icônes et messages suivants :

Icône	Affichage d'état	Description
	Protection Web	Si vous déplacez le curseur de la souris sur l'icône, le message suivant s'affiche : *La Protection Web d'Avira est activée. Votre navigation est securisée.* Aucune autre action n'est donc requise.
	Protection Web désactivée	Si vous déplacez le curseur de la souris sur l'icône, le message suivant s'affiche : *La Protection Web d'Avira est désactivée. Cliquez ici pour découvrir comment l'activer.* ↳ Vous êtes redirigé vers un article de notre base de connaissances.

⛔	*Protection Web non installée*	Si vous déplacez le curseur de la souris sur l'icône, le message suivant s'affiche : • *La Protection Web d'Avira n'est pas installée sur cet appareil. Cliquez ici pour découvrir comment sécuriser votre navigation.* Cela signifie que vous avez désinstallé l'antivirus Avira ou qu'il n'est pas installé correctement. • *Avec Avira Antivirus, vous bénéficiez gratuitement de Protection Web. Cliquez ici pour découvrir comment l'installer.* Cela signifie que vous n'avez pas installé la protection Web ou que vous l'avez désinstallée. ↳ Dans les deux cas, vous êtes redirigé sur la page Web d'Avira sur laquelle vous pouvez télécharger votre produit Avira.
?	*Erreur*	Si vous déplacez le curseur de la souris sur l'icône, le message suivant s'affiche : *Avira a signalé une erreur.* ▸ Cliquez sur l'icône grise ou sur le texte pour accéder à la page de support Avira.

Widgets

L'Avira SearchFree Toolbar dispose de 3 widgets avec les principales fonctions d'Internet : Facebook, messagerie électronique et protection Web.

Facebook

Cette fonction vous permet de recevoir directement les messages Facebook et donc de rester toujours au courant.

E-mail

Si vous cliquez sur l'icône e-mail, une liste déroulante s'affiche et vous permet de sélectionner parmi les principales messageries.



Protection Web

Ce widget a été développé par Avira et permet d'accéder très simplement à toutes les options de sécurité Internet. Pour le moment, il n'est disponible qu'avec Firefox et Internet Explorer. Différentes options sont proposées, elles peuvent porter des noms différents selon le navigateur :

- *Blocage des pop-up*

Si cette option est activée, toutes les fenêtres pop-up sont bloquées lorsque vous naviguez sur Internet.

- *Blocage des cookies*

Si cette option est activée, aucun cookie n'est enregistré pendant la navigation.

- *Mode privé (Firefox) / Navigation InPrivate (Internet Explorer)*

Si cette option est activée, vous ne laissez aucune trace lorsque vous naviguez sur Internet. Cette option n'est pas disponible pour Internet Explorer 7 et 8.

- *Supprimer l'historique récent (Firefox) / Supprimer l'historique de navigation (Internet Explorer)*

Cette option vous permet de supprimer toutes les activités Internet actuelles.

Conseiller en sécurité

Le conseiller en sécurité vous propose des niveaux de sécurité pendant que vous naviguez sur Internet.
Vous pouvez ainsi évaluer si le site que vous consultez présente un risque élevé ou faible pour votre sécurité.
Ce widget vous fournit des informations concernant le site Internet, comme le propriétaire du domaine, ou la raison du niveau de sécurité.
On compte trois niveaux de sécurité : sûr, peu risqué et très risqué.

Les niveaux de sécurité s'affichent dans la barre d'outils et dans les résultats de recherche sous la forme d'une icône de barre d'état Avira avec différents symboles :

Icône	Affichage d'état	Description
	Sûr	Une coche verte pour les sites Internet les plus sûrs.
	Risqué faible	Un point d'exclamation jaune pour les sites Internet qui présentent un risque faible.

	Risque élevé	Un panneau stop rouge pour les sites Internet présentant un risque élevé pour votre sécurité.
	Manqué	Un point d'interrogation gris pour les sites Internet dont le risque ne peut être évalué.
	Vérifier	Ce symbole s'affiche pendant la vérification de l'état.

Bloqueur de suivi

Le bloqueur de suivi vous permet d'interrompre le suivi et d'empêcher toute collecte d'informations lorsque vous naviguez sur Internet.
Le widget vous permet de sélectionner le suivi à bloquer et à autoriser.

Les entreprises se divisent en trois catégories :

- Réseaux sociaux
- Réseaux
- Autres entreprises

4.2.2 Options

L'Avira SearchFree Toolbar est compatible avec Internet Explorer, Firefox et Google Chrome, et peut être configurée à votre gré dans les navigateurs Web :

- Options de configuration Internet Explorer
- Options de configuration Firefox
- Options de configuration Chrome

Internet Explorer

Dans le navigateur Internet Explorer, vous disposez des options de configuration suivantes pour l'Avira SearchFree Toolbar dans le menu **Options** :

Options de Toolbar

Recherche

Sélectionner moteur Avira

Dans le menu **Sélectionner moteur Avira**, vous pouvez sélectionner le moteur de recherche à utiliser pour les recherches. Vous avez le choix entre des moteurs de recherche de différents pays : États-Unis, Brésil, Allemagne, Espagne, Europe, France, Italie, Pays-Bas, Russie et Grande-Bretagne.

Ouvrir recherches dans

Dans le menu de l'option **Ouvrir recherches dans**, vous pouvez sélectionner où afficher le résultat de la recherche, dans la **Fenêtre actuelle**, dans une **Nouvelle fenêtre** ou dans un **Nouvel onglet**.

Afficher les recherches récentes

Si l'option **Afficher les recherches récentes** est activée, vous pouvez demander l'affichage des termes saisis jusqu'alors sous le champ de saisie de la barre de recherche.

Supprimer historique des recherches en quittant le navigateur

Activez l'option **Supprimer historique des recherches en quittant le navigateur** si vous ne souhaitez pas enregistrer l'historique des recherches déjà effectuées mais si vous préférez les effacer lors de la fermeture du navigateur Web.

Autres options

Langue de Toolbar

Sous **Langue de Toolbar**, vous pouvez sélectionner la langue d'affichage de l'Avira SearchFree Toolbar. Vous avez le choix entre l'anglais, l'allemand, l'espagnol, le français, l'italien, le portugais et le néerlandais.

> **Remarque**
> La langue prédéfinie de l'Avira SearchFree Toolbar correspond à celle de votre programme, si elle est disponible. Si la barre d'outils n'est pas disponible dans votre langue, l'anglais est défini par défaut.

Afficher le texte des boutons

Désactivez l'option **Afficher le texte des boutons** si vous souhaitez masquer le texte à côté des icônes de l'Avira SearchFree Toolbar.

Supprimer l'historique

Activez l'option **Supprimer l'historique**, si vous ne souhaitez pas enregistrer la/les recherche(s) déjà effectué(es) mais préférez la/les supprimer immédiatement.

Aide

Cliquez sur **Aide** pour accéder au site Web et aux questions fréquentes (FAQ) sur la barre d'outils.

Désinstaller

Vous pouvez également désinstaller directement l'Avira SearchFree Toolbar sur Internet Explorer : Désinstallation via le navigateur Web.

A propos

Cliquez sur **A propos** pour afficher la version de l'Avira SearchFree Toolbar installée.

Firefox

Dans le navigateur Firefox, vous disposez des options de configuration suivantes pour l'Avira SearchFree Toolbar dans le menu **Options** :

Options de Toolbar

Recherche

Sélectionner moteur Avira

Dans le menu **Sélectionner moteur Avira**, vous pouvez sélectionner le moteur de recherche à utiliser pour les recherches. Vous avez le choix entre des moteurs de recherche de différents pays : États-Unis, Brésil, Allemagne, Espagne, Europe, France, Italie, Pays-Bas, Russie et Grande-Bretagne.

Afficher les recherches récentes

Si l'option **Afficher les recherches récentes** est activée, vous pouvez demander l'affichage des termes saisis jusqu'alors en cliquant sur la flèche dans la barre de recherche. Sélectionnez l'un des termes si vous souhaitez afficher de nouveau les résultats de recherche.

Supprimer historique des recherches en quittant le navigateur

Activez l'option **Supprimer historique des recherches en quittant le navigateur** si vous ne souhaitez pas enregistrer l'historique des recherches déjà effectuées mais si vous préférez les effacer lors de la fermeture du navigateur Web.

Afficher les résultats de recherches d'Ask lorsque je tape des mots-clés ou des URL non valides dans la barre d'adresse du navigateur

Si cette option est activée, chaque fois que vous saisissez des mots-clés ou une adresse URL non valide dans le champ d'adresse du navigateur Web, une recherche est lancée et les résultats s'affichent.

Autres options

Langue de Toolbar

Sous **Langue de Toolbar**, vous pouvez sélectionner la langue d'affichage de l'Avira SearchFree Toolbar. Vous avez le choix entre l'anglais, l'allemand, l'espagnol, le français, l'italien, le portugais et le néerlandais.

> **Remarque**
> La langue prédéfinie de l'Avira SearchFree Toolbar correspond à celle de votre programme, si elle est disponible. Si la barre d'outils n'est pas disponible dans votre langue, l'anglais est défini par défaut.

Afficher le texte des boutons

Désactivez l'option **Afficher le texte des boutons** si vous souhaitez masquer le texte à côté des icônes de l'Avira SearchFree Toolbar.

Supprimer l'historique

Activez l'option **Supprimer l'historique**, si vous ne souhaitez pas enregistrer la/les recherche(s) déjà effectué(es) mais préférez la/les supprimer immédiatement.

Aide

Cliquez sur **Aide** pour accéder au site Web et aux questions fréquentes (FAQ) sur la barre d'outils.

Désinstaller

Vous pouvez également désinstaller directement l'Avira SearchFree Toolbar sur Internet Explorer : Désinstallation via le navigateur Web.

A propos

Cliquez sur **A propos** pour afficher la version de l'Avira SearchFree Toolbar installée.

Chrome

Toutes les options de configuration sous le parapluie rouge Avira se trouvent dans le navigateur Web Google Chrome. Vous disposez des options suivantes pour l'Avira SearchFree Toolbar :

Aide

Cliquez sur **Aide** pour accéder au site Web et aux questions fréquentes (FAQ) sur la barre d'outils.

Instructions de désinstallation

Des liens vers les instructions de désinstallation de l'Avira SearchFree Toolbar sont disponibles ici.

A propos

Cliquez sur **A propos** pour afficher la version de l'Avira SearchFree Toolbar installée.

Afficher et masquer l'Avira SearchFree Toolbar

Cette option de menu permet de masquer et d'afficher l'Avira SearchFree Toolbar qui se trouve dans la partie supérieure de la fenêtre.

4.2.3 Désinstallation

Voici la procédure à suivre pour désinstaller votre Avira SearchFree Toolbar (sur l'exemple de Windows 7) :

- Ouvrez le **Panneau de configuration** via le menu **Démarrer** de Windows.
- Double-cliquez sur **Programmes et fonctionnalités**.
- Sélectionnez **Avira SearchFree Toolbar plus Web Protection** dans la liste et cliquez sur **Désinstaller**.
  - ↳ Un message vous demande alors si vous souhaitez vraiment désinstaller ce produit.
- Confirmez avec **Oui**.
  - ↳ L'Avira SearchFree Toolbar plus Web Protection sont désinstallées, votre ordinateur est redémarré si besoin est, et tous les répertoires, fichiers ainsi que toutes les entrées de Registre de l'Avira SearchFree Toolbar plus Web Protection sont supprimés.

Désinstallation via le navigateur Web

Vous avez également la possibilité de désinstaller l'Avira SearchFree Toolbar directement dans le navigateur avec **Firefox et Internet Explorer** :

- Ouvrez le menu **Options** à droite dans la barre de recherche.
- Cliquez sur **Désinstaller**.
  - ↳ Si votre navigateur Web est encore ouvert, un message vous demandera de le fermer.
- Fermez le navigateur et cliquez sur **OK**.
  - ↳ L'Avira SearchFree Toolbar plus Web Protection sont désinstallées, votre ordinateur est redémarré si besoin est, et tous les répertoires, fichiers ainsi que toutes les entrées de Registre de l'Avira SearchFree Toolbar plus Web Protection sont supprimés.

> **Remarque** Notez que pour la désinstallation de l'Avira SearchFree Toolbar, la barre d'outils doit être activée dans le gestionnaire de modules complémentaires.

Désinstallation en tant que module complémentaire

Étant donné que la dernière version de l'Avira SearchFree Toolbar est installée sous forme de module complémentaire, il est également possible de gérer l'outil avec différents gestionnaires de modules complémentaires.

Firefox

Cliquez sur **Outils > Modules complémentaires > Extensions**. Vous pouvez y gérer le module complémentaire d'Avira, c'est-à-dire l'activer, le désactiver ou le désinstaller.

Internet Explorer

Cliquez sur **Gérer les modules complémentaires > Barres d'outils et extensions**. Vous pouvez alors activer, désactiver et désinstaller le module complémentaire d'Avira.

Google Chrome

En cliquant sur **Outils > Extensions**, vous pouvez gérer le module complémentaire d'Avira. Cela vous permet d'activer, de désactiver ou de désinstaller la barre d'outils.

4.3 Comment procéder

Les chapitres « Comment procéder » vous fournissent une rapide description de la procédure d'activation de la licence et du produit ainsi que des principales fonctions de votre produit Avira. Les courts descriptifs sélectionnés vous permettent d'obtenir rapidement un aperçu des fonctionnalités de votre produit Avira. Ils ne remplacent toutefois pas les explications détaillées fournies dans les différents chapitres de cette Aide.

4.3.1 Activer la licence

Pour activer la licence de votre produit Avira, procédez de la manière suivante :

Avec le fichier de licence *.KEY*, vous activez votre licence pour votre produit Avira. Vous recevez votre fichier de licence par e-mail. Le fichier de licence contient la licence pour tous les produits que vous avez commandés.

Si vous n'avez pas encore installé votre produit Avira :

- Enregistrez le fichier de licence dans un répertoire local de votre ordinateur.
- Installez votre produit Avira.
- Lors de l'installation, indiquez où vous avez enregistré le fichier de licence.

Si vous avez déjà installé votre produit Avira :

- Double-cliquez dans votre gestionnaire de fichiers ou dans l'e-mail d'activation sur le fichier de licence et suivez les instructions à l'écran du gestionnaire de licences qui s'affiche.

  \- OU -

  Dans le Control Center de votre produit Avira, sélectionnez l'entrée de menu **Aide > Gestion des licences**

> **Remarque**
> Sous Windows Vista, la boîte de dialogue du **Contrôle du compte d'utilisateur** s'affiche. Connectez-vous comme administrateur le cas échéant. Cliquez sur **Continuer**.

- Sélectionnez le fichier de licence et cliquez sur **Ouvrir**.
  - ↳ Un message s'affiche.
- Validez avec **OK**.
  - ↳ La licence est activée.
- Redémarrez le système si nécessaire.

4.3.2 Activer le produit

Pour activer votre produit Avira, vous disposez des options suivantes :

- Activation avec une licence complète valide

  Pour activer le programme avec une licence complète, vous avez besoin d'un code d'activation valide, par le biais duquel les données de votre licence sont enregistrées. Soit nous vous avons envoyé le code d'activation par e-mail, soit celui-ci est indiqué sur l'emballage du produit.

- Activation avec une licence d'évaluation

  Votre produit Avira est activé par une licence d'évaluation générée automatiquement, grâce à laquelle vous pouvez tester l'intégralité des fonctions de votre produit Avira pendant une période limitée.

> **Remarque**
> Vous avez besoin d'une connexion Internet active pour activer le produit ou demander une licence test.
> Si aucune connexion ne peut être établie avec les serveurs Avira, vérifiez le cas échéant les paramètres du pare-feu utilisé : lors de l'activation du produit, les connexions sont établies via le protocole HTTP et le port 80 (communication) et via le protocole de cryptage SSL et le port 443. Assurez-vous que votre pare-feu ne bloque pas les données entrantes et sortantes. Vérifiez ensuite que vous pouvez accéder à des sites Internet par le biais de votre navigateur Web.

Pour activer votre produit Avira, procédez de la façon suivante :

Si vous n'avez pas encore installé votre produit Avira :

- Installez votre produit Avira.
  - ↳ Au cours de l'installation, vous êtes invité à choisir une option d'activation.
- **Activer le produit** = activation avec une licence complète valide

- **Tester le produit** = activation avec une licence d'évaluation

- Indiquez le code d'activation dans le cas d'une activation avec licence complète.
- Confirmez la sélection du processus d'activation en cliquant sur **Suivant**.
- Entrez vos données personnelles pour vous inscrire, le cas échéant, et confirmez votre saisie en cliquant sur **Suivant**.
  - ↳ Vos données de licence s'affichent dans la fenêtre de dialogue suivante. Votre produit Avira est activé.
- Poursuivez l'installation.

Si vous avez déjà installé votre produit Avira :

- Dans le Control Center, sélectionnez la rubrique **Aide > Gestion des licences**.
  - ↳ L'assistant de licence s'affiche, dans lequel vous pouvez choisir une option d'activation. Les étapes suivantes de l'activation du produit sont identiques à celles de la procédure présentée ci-avant.

4.3.3 Effectuer des mises à jour automatiques

Pour créer une tâche de mise à jour automatique de votre produit Avira avec le planificateur Avira, procédez de la façon suivante :

- Dans le Control Center, sélectionnez la rubrique *ADMINISTRATION* **> Planificateur**.
- Cliquez sur l'icône + **Créer une nouvelle tâche avec l'assistant**.
  - ↳ La boîte de dialogue **Nom et description de la tâche** s'affiche.
- Nommez la tâche et décrivez-la si besoin est.
- Cliquez sur **Suivant**.
  - ↳ La boîte de dialogue **Type de tâche** s'affiche.
- Sélectionnez **Tâche de mise à jour** dans la liste de sélection.
- Cliquez sur **Suivant**.
  - ↳ La boîte de dialogue **Heure de la tâche** s'affiche.
- Sélectionnez quand la mise à jour doit être effectuée :

- **Immédiatement**
- **Tous les jours**
- **Toutes les semaines**
- **Par intervalle**
- **Une fois**
- **Connexion**

Remarque
Nous vous recommandons d'effectuer des mises à jour régulières. L'intervalle de mise à jour recommandé est : 2 heures.

- Le cas échéant, saisissez la date selon votre sélection.
- Le cas échéant, sélectionnez des options supplémentaires (disponibles en fonction du type de tâche) :

- **Rattraper la tâche quand la date est déjà passée**
  Le programme effectue les tâches antérieures qui n'ont pas pu être exécutées au moment voulu, par ex. parce que l'ordinateur était éteint.
- **Démarrer également la tâche quand une connexion Internet est établie**
  Outre la fréquence définie, la tâche est exécutée à chaque démarrage d'une connexion Internet.

- Cliquez sur **Suivant**.
  ↳ La boîte de dialogue **Affichage de la fenêtre** s'affiche.
- Sélectionnez le mode d'affichage de la fenêtre des tâches :

- **Invisible** : pas de fenêtre des tâches
- **Réduit** : uniquement la barre de progression
- **Agrandi** : fenêtre des tâches complète

- Cliquez sur **Terminer**.
  ↳ La tâche que vous venez de créer apparaît comme activée (cochée) sur l'écran principal de la rubrique *ADMINISTRATION* **> Planificateur**.
- Désactivez éventuellement les tâches qui ne doivent pas être exécutées.

Les icônes suivantes vous permettent de continuer à modifier les tâches :

Afficher les propriétés d'une tâche

Modifier la tâche

Supprimer la tâche

Démarrer la tâche

Arrêter la tâche



4.3.4 Démarrer manuellement une mise à jour

Vous avez différentes possibilités de démarrer manuellement une mise à jour : une mise à jour du fichier de définitions des virus et du moteur de recherche est effectuée systématiquement dans le cas d'une mise à jour lancée manuellement.

Pour démarrer manuellement la mise à jour de votre produit Avira, procédez de la façon suivante :

- Avec le bouton droit de la souris, cliquez sur l'icône de la barre d'état Avira dans la barre des tâches et sélectionnez **Démarrer mise à jour**.

  \- OU -

- Dans le Control Center, sélectionnez la rubrique **État**, puis cliquez dans la zone **Dernière mise à jour** sur le lien **Démarrer mise à jour**.

  \- OU -

  Dans le menu **Mise à jour** du Control Center, sélectionnez la rubrique **Démarrer mise à jour**.

  ↳ La boîte de dialogue **Updater** s'affiche.

> **Remarque**
> Nous vous recommandons d'effectuer des mises à jour régulières. L'intervalle de mise à jour recommandé est : 2 heures.

> **Remarque**
> Vous pouvez également effectuer une mise à jour manuelle directement à partir du centre de sécurité Windows.

4.3.5 Recherche directe : chercher des virus et logiciels malveillants avec un profil de recherche

Un profil de recherche est un regroupement de lecteurs et répertoires à parcourir.

Pour rechercher via un profil de recherche, vous disposez des possibilités suivantes :

- Utiliser un profil de recherche prédéfini

  Si les profils de recherche prédéfinis répondent à vos besoins.

- Adapter et utiliser un profil de recherche (sélection manuelle)

  Si vous souhaitez chercher avec un profil de recherche individualisé.

- Créer et utiliser un nouveau profil de recherche

  Si vous souhaitez créer votre propre profil de recherche.

Selon le système d'exploitation, différentes icônes sont disponibles pour le démarrage d'un profil de recherche :

- Sous Windows XP :

  Cette icône vous permet de lancer la recherche via un profil de recherche.

- Sous Windows Vista :

  Sous Microsoft Windows Vista, le Control Center n'a d'abord que des droits restreints, par ex. pour l'accès aux répertoires et fichiers. Le Control Center ne peut exécuter certaines actions et accéder aux fichiers qu'avec des droits d'administrateur étendus. Ces droits d'administrateur étendus doivent être attribués à chaque démarrage d'une recherche via un profil de recherche.

  À l'aide de cette icône, vous démarrez une recherche limitée via un profil de recherche. Seuls les répertoires et fichiers pour lesquels Windows Vista a attribué les droits d'accès sont parcourus.

  À l'aide de cette icône, vous démarrez la recherche avec des droits d'administrateur étendus. Après confirmation, tous les répertoires et fichiers dans le profil de recherche sélectionné sont parcourus.

Pour chercher des virus et logiciels malveillants avec un profil de recherche, procédez de la façon suivante :

- Dans le Control Center, choisissez la rubrique *SÉCURITÉ PC* **> Scanner**.

  ↳ Les profils de recherche prédéfinis apparaissent.

- Sélectionnez l'un des profils de recherche prédéfinis.

  \- OU -

  Adaptez le profil de recherche **Sélection manuelle**.

  \- OU -

  Créez un nouveau profil de recherche

- Cliquez sur l'icône (Windows XP : ou Windows Vista :).
- La fenêtre **Luke Filewalker** s'affiche et la recherche directe démarre.

  ↳ À la fin du processus de recherche, les résultats s'affichent.

Si vous souhaitez adapter un profil de recherche :

- Dans le profil de recherche **Sélection manuelle**, déployez l'arborescence des fichiers de façon à ce que tous les lecteurs et les répertoires devant être parcourus soient ouverts

  - Cliquez sur le caractère **+** : le niveau de répertoire suivant s'affiche.
  - Cliquez sur le caractère **-** : le niveau de répertoire suivant est masqué.

- Sélectionnez les nœuds et les répertoires devant être parcourus, en cliquant sur chaque case correspondant à chaque niveau de répertoire

Pour sélectionner les répertoires, vous disposez des possibilités suivantes :

- Répertoire avec ses sous-répertoires (coche noire)
- Uniquement les sous-répertoires d'un répertoire (coche grise, les sous-répertoires ont une coche noire)
- Aucun répertoire (pas de coche)

Si vous souhaitez créer un nouveau profil de recherche :

- Cliquez sur l'icône **Créer un nouveau profil.**
  - ↪ Le profil *Nouveau profil* apparaît sous les profils existants.
- Renommez le profil de recherche si nécessaire, en cliquant sur l'icône .
- Sélectionnez les nœuds et répertoires à contrôler en cliquant une fois dans la case du niveau de répertoire concerné.

  Pour sélectionner les répertoires, vous disposez des possibilités suivantes :

- Répertoire avec ses sous-répertoires (coche noire)
- Uniquement les sous-répertoires d'un répertoire (coche grise, les sous-répertoires ont une coche noire)
- Aucun répertoire (pas de coche)

4.3.6 Recherche directe : chercher des virus et logiciels malveillants par glisser-déplacer

Pour chercher des virus et logiciels malveillants de manière ciblée par glisser-déplacer, procédez de la manière suivante :

- ✓ Ouvrez le Control Center de votre programme Avira.
- Sélectionnez le fichier ou le répertoire, qui doit être contrôlé.
- Avec le bouton gauche de la souris, faites glisser le fichier ou le répertoire sélectionné dans le Control Center.
  - ↪ La fenêtre **Luke Filewalker** s'affiche et la recherche directe démarre.
  - ↪ À la fin du processus de recherche, les résultats s'affichent.

4.3.7 Recherche directe : chercher des virus et logiciels malveillants via le menu contextuel

Pour rechercher des virus et des logiciels malveillants de manière ciblée via le menu contextuel, procédez de la façon suivante :

- Cliquez (par ex. dans l'explorateur Windows, sur le Bureau ou dans un répertoire Windows ouvert) avec le bouton droit de la souris sur le fichier ou le répertoire, que vous souhaitez contrôler.

↳ Le menu contextuel de l'explorateur Windows s'affiche.

- Dans le menu contextuel, sélectionnez **Contrôler les fichiers sélectionnés avec Avira**.

↳ La fenêtre **Luke Filewalker** s'affiche et la recherche directe démarre.

↳ À la fin du processus de recherche, les résultats s'affichent.

4.3.8 Recherche directe : recherche automatisée de virus et logiciels malveillants

> **Remarque**
> Après l'installation, la tâche de contrôle *Contrôle intégral du système* est créée dans le planificateur : un contrôle intégral du système est effectué dans l'intervalle recommandé.

Pour créer une tâche de recherche automatisée des virus et logiciels malveillants, procédez de la façon suivante :

- Dans le Control Center, sélectionnez la rubrique *ADMINISTRATION* **> Planificateur**.
- Cliquez sur l'icône + **Créer une nouvelle tâche avec l'assistant**.

↳ La boîte de dialogue **Nom et description de la tâche** s'affiche.

- Nommez la tâche et décrivez-la si besoin est.
- Cliquez sur **Suivant**.

↳ La boîte de dialogue **Type de tâche** s'affiche.

- Sélectionnez la **tâche de contrôle**.
- Cliquez sur **Suivant**.

↳ La boîte de dialogue **Sélection du profil** s'affiche.

- Choisissez le profil qui doit être parcouru.
- Cliquez sur **Suivant**.

↳ La boîte de dialogue **Heure de la tâche** s'affiche.

- Sélectionnez quand la recherche doit être effectuée :

- **Immédiatement**
- **Tous les jours**
- **Toutes les semaines**
- **Par intervalle**
- **Une fois**
- **Connexion**

- Le cas échéant, saisissez la date selon votre sélection.

- Sélectionnez l'option complémentaire le cas échéant (uniquement disponible en fonction du type de tâche) : **Rattraper la tâche quand la date est déjà passée**
  - ↳ Le programme effectue les tâches antérieures qui n'ont pas pu être exécutées au moment voulu, par ex. parce que l'ordinateur était éteint.
- Cliquez sur **Suivant**.
  - ↳ La boîte de dialogue **Affichage de la fenêtre** s'affiche.
- Sélectionnez le mode d'affichage de la fenêtre des tâches :

- **Invisible** : pas de fenêtre des tâches
- **Réduit** : uniquement la barre de progression
- **Agrandi** : fenêtre des tâches complète

- Sélectionnez l'option **Arrêter l'ordinateur quand la tâche a été exécutée**, si vous souhaitez que l'ordinateur s'arrête automatiquement dès que la tâche est exécutée et terminée.

  L'option est disponible uniquement en mode d'affichage de la fenêtre agrandi ou réduit.
- Cliquez sur **Terminer**.
  - ↳ La tâche que vous venez de créer apparaît comme activée (cochée) sur l'écran principal de la rubrique *ADMINISTRATION* **> Planificateur**.
- Désactivez éventuellement les tâches qui ne doivent pas être exécutées.

Les icônes suivantes vous permettent de continuer à modifier les tâches :

Afficher les propriétés d'une tâche

Modifier la tâche

Supprimer la tâche

Démarrer la tâche

Arrêter la tâche

4.3.9 Recherche directe : chercher les rootkits actifs de manière ciblée

Pour rechercher les rootkits actifs, utilisez le profil de recherche prédéfini **Recherche des rootkits et des logiciels malveillants actifs**.

Pour rechercher les rootkits actifs de manière ciblée, procédez de la façon suivante :

- Dans le Control Center, choisissez la rubrique *SÉCURITÉ PC* **> Scanner**.

↳ Les profils de recherche prédéfinis s'affichent.

- Sélectionnez le profil de recherche prédéfini **Recherche des rootkits et des logiciels malveillants actifs**.
- Sélectionnez les éventuels autres nœuds et répertoires à contrôler en cliquant dans la case du niveau de répertoire concerné.
- Cliquez sur l'icône (Windows XP : ou Windows Vista :).

↳ La fenêtre **Luke Filewalker** s'affiche et la recherche directe démarre.

↳ À la fin du processus de recherche, les résultats s'affichent.

4.3.10 Réagir aux virus et logiciels malveillants détectés

Pour les différents composants de protection de votre produit Avira, vous pouvez régler sous la rubrique **Action si résultat positif** la façon dont votre produit Avira doit réagir en cas de détection d'un virus ou d'un programme indésirable.

Pour le composant ProActiv de la protection temps réel, il n'y a aucune option d'action configurable : un résultat positif est toujours signalé dans la fenêtre **Protection temps réel : découverte d'un comportement suspect d'une application**.

Options d'action pour le scanner :

- **Interactif**

  En mode d'action interactif, les résultats positifs de la recherche du scanner sont signalés dans une boîte de dialogue. Ce paramètre est activé par défaut.
  Lors de la **recherche du scanner**, vous recevez à l'issue de la recherche un message d'avertissement comportant une liste des fichiers contaminés qui ont été trouvés. Vous avez la possibilité de sélectionner une action à exécuter pour les différents fichiers concernés, via le menu contextuel. Vous pouvez exécuter les actions choisies pour tous les fichiers concernés ou quitter le scanner.

- **Automatique**

  En mode d'action automatique, l'action que vous avez choisie dans cette zone est exécutée automatiquement en cas de détection d'un virus ou d'un programme indésirable.

Options d'action pour la protection temps réel :

- **Interactif**

  En mode d'action interactif, l'accès aux données est refusé et une notification s'affiche sur le Bureau. Dans la notification affichée sur le Bureau, vous avez la possibilité de supprimer le logiciel malveillant trouvé, ou de le transmettre au composant Scanner via le bouton **Détails** pour un traitement du virus. Le scanner signale le résultat positif dans une fenêtre où un menu contextuel vous propose différentes options pour traiter le fichier concerné (voir Résultat positif > Scanner).

- **Automatique**

En mode d'action automatique, l'action que vous avez choisie dans cette zone est exécutée automatiquement en cas de détection d'un virus ou d'un programme indésirable.

Options d'actions pour la protection e-mail et la protection Web :

- **Interactif**

  En mode d'action interactif, une boîte de dialogue s'affiche en cas de détection d'un virus ou d'un programme indésirable, vous permettant de choisir ce qu'il doit advenir de l'objet concerné. Ce paramètre est activé par défaut.

- **Automatique**

  En mode d'action automatique, l'action que vous avez choisie dans cette zone est exécutée automatiquement en cas de détection d'un virus ou d'un programme indésirable.

Mode d'action interactif

▶ En mode d'action interactif, vous réagissez aux virus et programmes indésirables détectés en sélectionnant dans le message une **Action pour les objets contaminés** et exécutez l'action en cliquant sur **Confirmer**.

Les actions de traitement des objets concernés suivantes sont disponibles :

> **Remarque**
> Les actions disponibles à la sélection dépendent du système d'exploitation, du composant de protection (Scanner Avira, Protection temps réel Avira, Protection e-mail Avira, Protection Web Avira) qui signale le résultat positif, et du logiciel malveillant détecté.

Actions du scanner et de la protection temps réel (sans résultat positif détecté par ProActiv) :

- **Réparer**

  Le fichier est réparé.
  Cette option n'est activable que si une réparation du fichier trouvé est possible.

- **Renommer**

  Le fichier est renommé en **.vir*. Un accès direct à ces fichiers (par un double clic par ex.) n'est alors plus possible. Les fichiers peuvent être réparés et renommés ultérieurement.

- **Quarantaine**

  Le fichier est compressé dans un format spécial (**.qua*) et déplacé dans le répertoire de quarantaine *INFECTED* sur votre disque dur pour empêcher tout accès direct. Les fichiers de ce répertoire peuvent ensuite être réparés en quarantaine ou - si nécessaire - envoyés à Avira.

- **Supprimer**

Le fichier est supprimé. Cette procédure est beaucoup plus rapide que le processus d'**écrasement et de suppression**.
Si le résultat positif est un virus de secteur d'amorçage, le secteur d'amorçage est effacé en cas de suppression. Un nouveau secteur d'amorçage est écrit.

- **Ignorer**

  Aucune action supplémentaire n'est effectuée. Le fichier concerné reste actif sur votre ordinateur.

- **Écraser et supprimer**

  Le fichier est écrasé par un modèle standard puis supprimé. Il ne peut plus être restauré.

> **Avertissement**
> Risque de perte de données et de dommages sur le système d'exploitation.
> Utilisez l'option **Ignorer** uniquement dans des cas exceptionnels le justifiant.

- **Toujours ignorer**

  Option d'action en cas de résultat positif avec la protection temps réel : aucune action supplémentaire n'est effectuée par la protection temps réel. L'accès au fichier est autorisé. Tous les accès ultérieurs à ce fichier sont autorisés et ne sont plus signalés jusqu'au redémarrage de l'ordinateur ou jusqu'à la mise à jour du fichier de définitions des virus.

- **Copier en quarantaine**

  Option d'action en cas de détection d'un rootkit : le programme trouvé est copié en quarantaine.

- **Réparer le secteur d'amorçage | Télécharger l'outil de réparation**

  Options d'action en cas de détection de secteurs d'amorçage infectés : des options d'action pour la réparation de lecteurs de disquettes sont disponibles. Si aucune réparation n'est possible avec votre produit Avira, vous pouvez télécharger un outil spécial pour la détection et la suppression de virus de secteur d'amorçage.

> **Remarque**
> Si vous appliquez des actions sur des processus en cours, les processus concernés sont arrêtés avant l'exécution de l'action.

Action de la protection temps réel en cas de résultat positif avec le composant ProActiv (message d'actions suspectes d'une application) :

- **Programme fiable**

  L'exécution de l'application se poursuit. Le programme est ajouté à la liste des applications autorisées, et il est exclu de la surveillance effectuée par le composant ProActiv. Lors de l'ajout à la liste des applications autorisées, le type de surveillance est définie sur *Contenu*. Cela signifie que l'application n'est exclue d'une surveillance

par le composant ProActiv que si le contenu reste inchangé (voir Filtre des applications : applications à exclure).

- **Bloquer le programme une fois**

  L'application est bloquée, c'est-à-dire que l'exécution de l'application est arrêtée. Le composant ProActiv continue à surveiller les actions de l'application.

- **Toujours bloquer ce programme**

  L'application est bloquée, c'est-à-dire que l'exécution de l'application est arrêtée. Le programme est ajouté à la liste des applications à bloquer et ne peut plus être exécuté (voir Filtre des applications : applications à bloquer).

- **Ignorer**

  L'exécution de l'application se poursuit. Le composant ProActiv continue à surveiller les actions de l'application.

Actions de la protection e-mail : e-mails entrants

- **Déplacer en quarantaine**

  L'e-mail, y compris toutes les pièces jointes, est déplacé en quarantaine. L'e-mail contaminé est supprimé. Le corps et les pièces jointes éventuelles de l'e-mail sont remplacés par un texte standard.

- **Supprimer l'e-mail**

  L'e-mail contaminé est supprimé. Le corps et les pièces jointes éventuelles sont remplacés par un texte standard.

- **Supprimer la pièce jointe**

  La pièce jointe contaminée est remplacée par un texte standard. Si le corps de l'e-mail est contaminé, celui-ci est supprimé et également remplacé par un texte standard. L'e-mail lui-même est délivré.

- **Déplacer la pièce jointe en quarantaine**

  La pièce jointe concernée est placée en quarantaine puis supprimée (remplacée par un texte standard). Le corps de l'e-mail est délivré. La pièce jointe contaminée peut être délivrée plus tard par le gestionnaire de quarantaines.

- **Ignorer**

  L'e-mail concerné est délivré.

> **Avertissement**
> Ce faisant, il est possible que des virus et programmes indésirables arrivent sur votre ordinateur. Choisissez l'option **Ignorer** uniquement dans des cas exceptionnels le justifiant. Désactivez l'aperçu dans Microsoft Outlook, n'ouvrez en aucun cas les pièces jointes par double-clic.

Actions de la protection e-mail : e-mails sortants

- **Déplacer l'e-mail en quarantaine (ne pas envoyer)**



L'e-mail, y compris toutes les pièces jointes, sont copiés dans la quarantaine et ne sont pas envoyés. L'e-mail reste dans la boîte d'envoi de votre client de messagerie. Vous recevez un message d'erreur dans votre programme de messagerie. La présence de logiciels malveillants est contrôlée dans cet e-mail à chaque processus d'envoi ultérieur de votre compte de messagerie.

- **Bloquer l'envoi d'e-mails (ne pas envoyer)**

  L'e-mail n'est pas envoyé et reste dans la boîte d'envoi de votre client de messagerie. Vous recevez un message d'erreur dans votre programme de messagerie. La présence de logiciels malveillants est contrôlée dans cet e-mail à chaque processus d'envoi ultérieur de votre compte de messagerie.

- **Ignorer**

  L'e-mail concerné est envoyé.

Avertissement
Ce faisant, il est possible que des virus et programmes indésirables arrivent sur l'ordinateur du destinataire de l'e-mail.

Actions de la protection Web :

- **Refuser l'accès**

  La page Web demandée par le serveur Web ou les données et fichiers transmis ne sont pas envoyés à votre navigateur Web. Un message d'erreur de refus d'accès s'affiche dans le navigateur Web.

- **Quarantaine**

  La page Web demandée par le serveur Web ou les données et fichiers transmis sont déplacés en quarantaine. Le fichier concerné peut être restauré depuis le gestionnaire de quarantaines s'il a une valeur informative ou, si nécessaire, être envoyé à l'Avira Malware Research Center.

- **Ignorer**

  La page Web demandée par le serveur Web ou les données et fichiers transmis sont envoyés à votre navigateur Web par la protection Web.

Avertissement
Ce faisant, il est possible que des virus et programmes indésirables arrivent sur votre ordinateur. Choisissez l'option **Ignorer** uniquement dans des cas exceptionnels le justifiant.

Remarque
Nous conseillons de déplacer en quarantaine un fichier suspect qui ne peut être réparé.

Remarque
Envoyez-nous également les fichiers signalés par l'heuristique pour analyse. Vous pouvez télécharger ces fichiers par ex. via notre site Web : http://www.avira.com/fr/sample-upload
Vous identifiez les fichiers signalés par l'heuristique à la désignation *HEUR/* ou *HEURISTIC/*, antéposée aux noms des fichiers, par ex : *HEUR/fichiers test.**.

4.3.11 Quarantaine : traiter les fichiers (*.qua) en quarantaine

Pour traiter les fichiers en quarantaine, procédez de la façon suivante :

- Dans le Control Center, sélectionnez la rubrique *ADMINISTRATION* **> Quarantaine**.
- Vérifiez de quels fichiers il s'agit pour pouvoir recharger les originaux d'un autre emplacement sur votre ordinateur, le cas échéant.

Si vous souhaitez afficher des informations plus détaillées sur un fichier :

- Sélectionnez le fichier et cliquez sur i.
  - ↳ La boîte de dialogue **Propriétés** s'affiche avec des informations supplémentaires sur le fichier.

Si vous souhaitez à nouveau contrôler un fichier :

La vérification d'un fichier est recommandée quand le fichier de définitions de virus de votre produit Avira a été actualisé et qu'il y a un doute de fausse alerte. De cette façon, vous pouvez confirmer une fausse alerte lors du nouveau contrôle et restaurer le fichier.

- Sélectionnez le fichier et cliquez sur .
  - ↳ L'absence de virus et logiciels malveillants est contrôlée sur le fichier avec les paramètres de la recherche directe.
  - ↳ Après le contrôle, la boîte de dialogue **Statistiques de contrôle** s'affiche avec les statistiques sur l'état du fichier avant et après le deuxième contrôle.

Si vous souhaitez supprimer un fichier :

- Sélectionnez le fichier et cliquez sur ✕.
- Confirmez votre sélection avec **Oui**.

Si vous souhaitez charger le fichier sur un serveur Web de l'Avira Malware Research Center en vue d'une analyse :

- Sélectionnez le fichier que vous souhaitez télécharger.
- Cliquez sur .

↳ La boîte de dialogue *Chargement du fichier* s'ouvre, avec un formulaire pour la saisie de vos coordonnées.

- Indiquez les données complètes.
- Sélectionnez un type : **Fichier suspect** ou **Doute de fausse alerte**.
- Sélectionnez un format de réponse : **HTML**, **Texte**, **HTML & texte**.
- Cliquez sur **OK.**

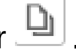
↳ Le fichier est chargé sur un serveur Web de l'Avira Malware Research Center.

Remarque
Dans les cas suivants, une analyse par l'Avira Malware Research Center est recommandée :
Résultat heuristique positif (fichier suspect) : lors d'une recherche, votre produit Avira a classé un fichier comme suspect et l'a placé en quarantaine : dans la boîte de dialogue de détection de virus ou dans le fichier rapport de la recherche, il a été recommandée de faire analyser le fichier par l'Avira Malware Research Center.
Fichier suspect : vous considérez un fichier comme suspect et l'avez de ce fait ajouté à la quarantaine, mais le contrôle du fichier quant à la présence de virus et de logiciels malveillants est négatif.
Doute de fausse alerte : vous supposez que la détection de virus est une fausse alerte : votre produit Avira signale la détection d'un virus dans un fichier, lequel n'est cependant, selon toute vraisemblance, pas infecté par un logiciel malveillant.

Remarque
La taille des fichiers que vous téléchargez est limitée à 20 Mo au format non compressé ou à 8 Mo en format compressé.

Remarque
Vous ne pouvez télécharger qu'un seul fichier à la fois.

Si vous souhaitez copier un objet en quarantaine dans un autre répertoire en le sortant de la quarantaine :

- Sélectionnez l'objet en quarantaine et cliquez sur .

↳ La boîte de dialogue *Rechercher le dossier* s'ouvre, dans laquelle vous pouvez sélectionner un répertoire.

- Sélectionnez un répertoire dans lequel une copie de l'objet en quarantaine doit être mémorisée et validez votre sélection avec **OK**.

↳ L'objet en quarantaine sélectionné est enregistré dans le répertoire sélectionné.

Remarque
L'objet en quarantaine n'est pas identique au fichier restauré. L'objet en quarantaine est codé et ne peut pas être exécuté ni lu dans le format d'origine.

Si vous souhaitez exporter les propriétés de l'objet en quarantaine dans un fichier texte :

- Sélectionnez l'objet en quarantaine et cliquez sur .
  ↳ Un fichier texte s'ouvre avec les données relatives à l'objet en quarantaine sélectionné.
- Enregistrez le fichier texte.

Vous pouvez également restaurer les fichiers en quarantaine (voir chapitre : Quarantaine : restaurer les fichiers en quarantaine).

4.3.12 Quarantaine : restaurer les fichiers en quarantaine

En fonction du système d'exploitation, diverses icônes sont disponibles pour la restauration :

- **Sous Windows XP et 2000** :

  Cette icône vous permet de restaurer les fichiers dans le répertoire d'origine.

  Cette icône vous permet de restaurer des fichiers dans un répertoire de votre choix.

- **Sous Windows Vista** :

  Sous Microsoft Windows Vista, le Control Center n'a d'abord que des droits restreints, par ex. pour l'accès aux répertoires et fichiers. Le Control Center ne peut exécuter certaines actions et accéder aux fichiers qu'avec des droits d'administrateur étendus. Ces droits d'administrateur étendus doivent être attribués à chaque démarrage d'une recherche via un profil de recherche.

  Cette icône vous permet de restaurer des fichiers dans un répertoire de votre choix.

  Cette icône vous permet de restaurer les fichiers dans le répertoire d'origine. Si des droits d'administrateur sont nécessaires pour accéder à ce répertoire, une demande s'affiche.

Pour restaurer des fichiers en quarantaine, procédez de la manière suivante :

Avertissement
Risque de perte de données et de dommages sur le système d'exploitation de

l'ordinateur. N'utilisez la fonction **Restaurer l'objet sélectionné** que dans des cas exceptionnels. Assurez-vous de ne restaurer que des fichiers qui ont pu être réparés au cours d'une nouvelle recherche.

✓ Fichier recontrôlé et réparé par une recherche.

- Dans le Control Center, sélectionnez la rubrique *ADMINISTRATION* **> Quarantaine**.

> **Remarque**
> Il n'est possible de restaurer les e-mails et pièces jointes d'e-mails qu'avec l'option et avec l'extension **.eml*.

Si vous souhaitez restaurer un fichier à son emplacement d'origine :

- Sélectionnez le fichier et cliquez sur l'icône (Windows XP : , Windows Vista).

Cette option n'est pas disponible pour les e-mails.

> **Remarque**
> Il n'est possible de restaurer les e-mails et pièces jointes d'e-mails qu'avec l'option et avec l'extension **.eml*.

↳ Le système vous demande si vous souhaitez restaurer le fichier.

- Cliquez sur **Oui**.

↳ Le fichier est restauré dans le répertoire à partir duquel il avait été placé en quarantaine.

Si vous souhaitez restaurer un fichier dans un répertoire particulier :

- Sélectionnez le fichier et cliquez sur .

↳ Le système vous demande si vous souhaitez restaurer le fichier.

- Cliquez sur **Oui**.

↳ La fenêtre Windows par défaut pour sélectionner un répertoire s'affiche.

- Sélectionnez le répertoire dans lequel le fichier doit être restauré et validez.

↳ Le fichier est restauré dans le répertoire choisi.

4.3.13 Quarantaine : déplacer un fichier suspect en quarantaine

Vous pouvez déplacer manuellement un fichier suspect en quarantaine de la manière suivante :

- Dans le Control Center, sélectionnez la rubrique *ADMINISTRATION* **> Quarantaine**.



- Cliquez sur [+].
  - ↳ La fenêtre standard Windows pour sélectionner un fichier s'affiche.
- Choisissez un fichier et validez avec **Ouvrir**.
  - ↳ Le fichier est déplacé en quarantaine.

Vous pouvez vérifier les fichiers en quarantaine avec le scanner Avira (voir chapitre : Quarantaine : traiter les fichiers (*.qua) en quarantaine).

4.3.14 Profil de recherche : compléter ou supprimer un type de fichier dans un profil de recherche

Voici comment établir pour un profil de recherche qui scanne des types de fichiers supplémentaires ou exclut certains types de fichiers lors de la recherche (possible uniquement en cas de sélection manuelle et de profils de recherche définis par l'utilisateur) :

✓ Dans le Control Center, accédez à la rubrique *SÉCURITÉ PC* **> Scanner**.

- Cliquez avec le bouton droit de la souris sur le profil de recherche que vous souhaitez éditer.
  - ↳ Un menu contextuel s'affiche.
- Sélectionnez l'entrée **Filtre de fichiers**.
- Déployez le menu contextuel en cliquant sur le petit triangle à droite du menu contextuel.
  - ↳ Les entrées **Standard**, **Contrôler tous les fichiers** et **Personnalisé** apparaissent.
- Sélectionnez l'entrée **Personnalisé**.
  - ↳ La boîte de dialogue **Extensions de fichiers** s'affiche avec une liste de tous les types de fichiers qui sont parcourus avec le profil de recherche.

Si vous voulez exclure un type de fichier de la recherche :

- Sélectionnez le type de fichier et cliquez sur **Supprimer**.

Si vous voulez ajouter un type de fichier à la recherche :

- Sélectionnez le type de fichier.
- Cliquez sur **Ajouter** et saisissez l'extension de fichier du type de fichier dans le champ de saisie.

  Utilisez au maximum 10 caractères et ne tapez pas le point initial. Les caractères de remplacement (* et ?) sont autorisés.

4.3.15 Profil de recherche : créer un raccourci sur le Bureau pour le profil de recherche

Le raccourci sur le Bureau vers un profil de recherche vous permet de démarrer une recherche directe depuis votre Bureau, sans accéder au Control Center de votre produit Avira.

Pour créer un raccourci vers le profil de recherche sur le Bureau, procédez de la manière suivante :

✓ Dans le Control Center, accédez à la rubrique *SÉCURITÉ PC* **> Scanner**.

- Sélectionnez le profil de recherche vers lequel vous souhaitez créer un raccourci.
- Cliquez sur l'icône .
  - ↳ Le raccourci sur le Bureau est créé.

4.3.16 Événements : filtrer les événements

Dans le Control Center, sous *ADMINISTRATION* **> Événements** sont affichés tous les événements générés par les composants programme de votre produit Avira (comme avec l'affichage des événements de votre système d'exploitation Windows). Les composants programme sont, par ordre alphabétique, les suivants :

- Sauvegarde
- Protection Web
- Protection temps réel
- Protection e-mail
- FireWall
- Service d'assistance
- Planificateur
- Navigation sécurisée
- Scanner
- Updater

Les types d'événements suivants s'affichent :

- *Information*
- *Avertissement*
- *Erreur*
- *Résultat positif*

Voici comment filtrer les événements affichés :

- Dans le Control Center, sélectionnez la rubrique *ADMINISTRATION* > Événements.

- Activez les cases à cocher des composants programme pour afficher les événements des composants activés.

  - OU -

  Décochez les cases à cocher des composants programme pour masquer les événements des composants désactivés.

- Activez la case à cocher des types d'événements pour afficher ces événements.

  - OU -

  Décochez les cases des types d'événements pour masquer ces événements.

4.3.17 Protection e-mail : exclure des adresses e-mail du contrôle

Pour exclure des adresses e-mail (expéditeur) du contrôle par la protection e-mail (mise sur liste blanche), procédez de la façon suivante :

- Dans le Control Center, sélectionnez la rubrique *SÉCURITÉ INTERNET* **> Protection e-mail**.

  ↳ Vous voyez dans la liste les e-mails reçus.

- Sélectionnez l'e-mail que vous souhaitez exclure du contrôle de la protection e-mail.
- Cliquez sur l'icône souhaitée pour exclure l'e-mail du contrôle par la protection e-mail :

  L'adresse e-mail sélectionnée ne sera plus contrôlée à l'avenir pour rechercher virus et programmes indésirables.

  L'adresse e-mail sélectionnée ne sera plus contrôlée à l'avenir pour rechercher des spams.

  ↳ L'adresse e-mail de l'expéditeur est ajoutée à la liste d'exceptions et n'est plus contrôlée quant à l'absence de virus et de logiciels malveillants ou de spam.

Avertissement
N'excluez du contrôle par la protection e-mail que les adresses e-mail absolument dignes de confiance.

Remarque
Dans la configuration, sous Protection e-mail > Généralités > Exceptions, vous pouvez intégrer des adresses e-mail supplémentaires dans la liste d'exceptions ou en supprimer.

4.3.18 Protection e-mail : entraîner le module AntiSpam

Le module AntiSpam contient une base de données d'apprentissage. Cette base de données d'apprentissage intègre vos critères individuels de catégorisation. Au fil du temps, les filtres internes, algorithmes et critères d'évaluation pour le spam s'ajustent à vos critères personnels.

Pour catégoriser les e-mails pour la base de données d'apprentissage, procédez de la façon suivante :

- Dans le Control Center, sélectionnez la rubrique *SÉCURITÉ INTERNET* **> Protection e-mail**.
  - ↳ Dans la liste, vous voyez les e-mails entrants.
- Sélectionnez l'e-mail à catégoriser.
- Cliquez sur l'icône souhaitée pour catégoriser l'e-mail par ex. comme *Spam* ou comme e-mail accepté (« *normal* ») .
  - ↳ L'e-mail est intégré dans la base de données d'apprentissage et sert à la détection de spam la prochaine fois.

> **Remarque**
> Vous pouvez supprimer la base de données d'apprentissage dans la configuration sous **Protection e-mail > Généralités > AntiSpam**.
>
> **Remarque**
> L'exclusion de certaines adresses e-mail du contrôle concernant les logiciels malveillants ne s'applique évidemment qu'aux e-mails entrants. Les fonctions d'apprentissage et les exceptions AntiSpam ne concernent également que les e-mails entrants. Pour désactiver le contrôle des e-mails sortants, désactivez cette fonction dans la configuration sous Protection e-mail > Recherche.

4.3.19 FireWall : choisir le niveau de sécurité du FireWall

Vous avez le choix entre plusieurs niveaux de sécurité. En fonction de cela, vous avez diverses possibilités de configuration pour les règles d'adaptation.

Les niveaux de sécurité suivants sont disponibles :

Bas

La saturation et le scannage des ports sont détectés.

Moyen

Les paquets TCP et UDP suspects sont rejetés.

La saturation et le scannage des ports sont empêchés.

(Paramètre par défaut)

Élevé

L'ordinateur est invisible dans le réseau.

Les nouvelles connexions de l'extérieur ne sont pas autorisées.

La saturation et le scannage des ports sont empêchés.

Utilisateur

Règles définies par l'utilisateur : le programme passe automatiquement à ce niveau de sécurité si vous avez modifié les règles d'adaptation.

Bloquer tout

Ferme toutes les connexions réseau existantes.

> **Remarque**
> Le paramètre par défaut du niveau de sécurité pour toutes les règles prédéfinies de l'Avira FireWall est **Moyen.**

Pour régler le niveau de sécurité du FireWall, procédez de la façon suivante :

- Dans le Control Center, sélectionnez la rubrique *SÉCURITÉ INTERNET* **> FireWall**.
- Placez le curseur sur le niveau de sécurité souhaité.
  - ↳ Le niveau de sécurité sélectionné est aussitôt activé.

4.3.20 Sauvegarde : créer manuellement des sauvegardes

L'outil de sauvegarde du Control Center vous permet de créer rapidement et simplement une sauvegarde de vos données personnelles. La sauvegarde Avira vous permet de créer des sauvegardes en miroir grâce auxquelles vous pouvez sauvegarder et conserver vos données à leur niveau le plus récent, sans utiliser trop de ressources. Lors de la sauvegarde à l'aide de la fonction d'Avira, l'absence de virus et de logiciels malveillants peut être contrôlée dans les fichiers à sauvegarder. Les fichiers contaminés ne sont pas sauvegardés.

> **Remarque**
> Contrairement à une sauvegarde de version, aucune version individuelle de sauvegarde n'est conservée lors d'une sauvegarde en miroir. La sauvegarde en miroir contient l'ensemble des données au moment de la dernière sauvegarde. Toutefois, si des fichiers sont effacés de l'ensemble des données à sauvegarder, aucune synchronisation n'est effectuée lors de la sauvegarde

suivante, c'est-à-dire que les fichiers supprimés se trouvent encore dans la sauvegarde.

Remarque
La sauvegarde Avira avec des paramètres par défaut sauvegarde uniquement les fichiers modifiés et un contrôle est effectué concernant les virus et logiciels malveillants. Vous pouvez modifier ces paramètres dans la configuration Sauvegarde > Paramètres.

Pour sauvegarder vos données à l'aide de l'outil de sauvegarde, procédez de la façon suivante :

- Dans le Control Center, sélectionnez la rubrique *SÉCURITÉ PC* **> Sauvegarde**.
  ↳ Les profils de sauvegarde prédéfinis s'affichent à l'écran.
- Sélectionnez l'un des profils de sauvegarde prédéfinis.

  - OU -

  Adaptez le profil de sauvegarde **Sélection manuelle** en fonction de vos besoins.

  - OU -

  Créez un nouveau profil de sauvegarde
- Indiquez un emplacement de sauvegarde dans le champ **Répertoire cible** pour le profil choisi.

  Vous pouvez choisir comme emplacement de sauvegarde un répertoire de votre ordinateur ou d'un lecteur réseau connecté ainsi qu'un support amovible tel qu'une clé USB ou une disquette.
- Cliquez sur l'icône .
  ↳ La fenêtre **Sauvegarde Avira** s'affiche à l'écran et la sauvegarde démarre. L'état et les événements de la sauvegarde s'affichent dans la fenêtre de sauvegarde.

Si vous souhaitez adapter un profil de sauvegarde :

- Dans le profil de recherche **Sélection manuelle**, ouvrez l'arborescence de manière à ce que tous les lecteurs et répertoires devant être sauvegardés soient ouverts :
- Cliquez sur le caractère **+** : le niveau de répertoire suivant s'affiche.
- Cliquez sur le caractère **-** : le niveau de répertoire suivant est masqué.
- Sélectionnez les nœuds et répertoires à sauvegarder en cliquant une fois dans la case des différents niveaux de répertoire concernés :

  Pour sélectionner les répertoires, vous disposez des possibilités suivantes :
- Répertoire avec ses sous-répertoires (coche noire)

- Uniquement les sous-répertoires d'un répertoire (coche grise, les sous-répertoires ont une coche noire)
- Aucun répertoire (pas de coche)

Si vous souhaitez créer un nouveau profil de sauvegarde :

- Cliquez sur l'icône **Créer un nouveau profil**.
  - ↳ Le profil *Nouveau profil* apparaît sous les profils existants.
- Renommez le profil de sauvegarde si nécessaire, en cliquant sur l'icône .
- Sélectionnez les nœuds et répertoires à sauvegarder en cliquant une fois dans la case du niveau de répertoire concerné.

  Pour sélectionner les répertoires, vous disposez des possibilités suivantes :

- Répertoire avec ses sous-répertoires (coche noire)
- Uniquement les sous-répertoires d'un répertoire (coche grise, les sous-répertoires ont une coche noire)
- Aucun répertoire (pas de coche)

4.3.21 Sauvegarde : créer des sauvegardes de données automatisées

Voici comment vous pouvez créer une tâche permettant d'effectuer des sauvegardes de données automatisées :

- Dans le Control Center, sélectionnez la rubrique *ADMINISTRATION* **> Planificateur**.
- Cliquez sur l'icône .
  - ↳ La boîte de dialogue **Nom et description de la tâche** s'affiche.
- Nommez la tâche et décrivez-la si besoin est.
- Cliquez sur **Suivant**.
  - ↳ La boîte de dialogue **Type de tâche** s'affiche.
- Sélectionnez l'entrée **Tâche de sauvegarde**.
- Cliquez sur **Suivant**.
  - ↳ La boîte de dialogue **Sélection du profil** s'affiche.
- Choisissez le profil qui doit être parcouru.

> **Remarque**
> Seuls s'affichent les profils de sauvegarde pour lesquels un emplacement de sauvegarde a été indiqué.

- Cliquez sur **Suivant**.

↳ La boîte de dialogue **Heure de la tâche** s'affiche.

- Sélectionnez quand la recherche doit être effectuée :

- **Immédiatement**
- **Tous les jours**
- **Toutes les semaines**
- **Par intervalle**
- **Une fois**
- **Connexion**
- **Plug&Play**

Pour l'événement **Plug&Play**, la sauvegarde est créée dès que le support d'échanges de données indiqué comme emplacement de sauvegarde pour le profil de sauvegarde est connecté à l'ordinateur. L'événement de sauvegarde **Plug&Play** implique qu'une clé USB a été indiquée comme emplacement de sauvegarde.

- Le cas échéant, saisissez la date selon votre sélection.
- Sélectionnez l'option complémentaire suivante le cas échéant (uniquement disponible en fonction du type de tâche) : **Rattraper la tâche quand la date est déjà passée**

↳ Le programme effectue les tâches antérieures qui n'ont pas pu être exécutées au moment voulu, par ex. parce que l'ordinateur était éteint.

- Cliquez sur **Suivant**.

↳ La boîte de dialogue **Affichage de la fenêtre** s'affiche.

- Sélectionnez le mode d'affichage de la fenêtre des tâches :

- **Réduit** : uniquement la barre de progression
- **Agrandi** : l'ensemble de la fenêtre de sauvegarde
- **Invisible** : pas de fenêtre de sauvegarde

- Cliquez sur **Terminer**.

↳ La tâche que vous venez de créer apparaît comme activée (cochée) sur l'écran principal de la rubrique *ADMINISTRATION* **> Planificateur**.

- Désactivez éventuellement les tâches qui ne doivent pas être exécutées.

Les icônes suivantes vous permettent de continuer à éditer les tâches :

Afficher les propriétés d'une tâche

Modifier la tâche

Supprimer la tâche

Démarrer la tâche

Arrêter la tâche

5. Scanner

Grâce au composant Scanner, vous pouvez rechercher de manière ciblée les virus et programmes indésirables (recherche directe). Vous avez les possibilités suivantes pour rechercher des fichiers contaminés :

- **Recherche directe via le menu contextuel**
  La recherche directe via le menu contextuel (bouton droit de la souris - entrée **Contrôler les fichiers sélectionnés avec Avira**) est recommandée si vous voulez contrôler des fichiers et répertoires séparément dans l'explorateur Windows par exemple. Un autre avantage est qu'il n'est pas nécessaire de démarrer le Control Center pour la recherche directe via le menu contextuel.
- **Recherche directe par glisser-déplacer**
  En glissant un fichier ou un répertoire dans la fenêtre de programme du Control Center, le scanner contrôle le fichier ou le répertoire, ainsi que tous les sous-répertoires inclus. Cette procédure est recommandée si vous souhaitez contrôler des fichiers et répertoires séparément, que vous avez par ex. déposés sur votre Bureau.
- **Recherche directe via les profils**
  Cette procédure est recommandée si vous souhaitez contrôler régulièrement certains répertoires et lecteurs (par ex. votre répertoire de travail ou les lecteurs sur lesquels vous déposez régulièrement des fichiers). Il n'est alors plus nécessaire de sélectionner ces répertoires et lecteurs à chaque contrôle, il suffit d'une simple sélection avec le profil correspondant.
- **Recherche directe via le planificateur**
  Le planificateur permet d'effectuer des tâches de contrôle programmées.

Des procédures particulières sont nécessaires lors de la recherche de rootkits, de virus de secteurs d'amorçage et du contrôle de processus actifs. Vous disposez des options suivantes :

- Recherche de rootkits via le profil de recherche **Recherche des rootkits et des logiciels malveillants actifs**
- Contrôle des processus actifs via le profil de recherche **Processus actifs**
- Recherche de virus de secteurs d'amorçage via la commande **Contrôler les virus de secteurs d'amorçage** dans le menu **Extras**

6. Mises à jour

L'efficacité d'un logiciel antivirus dépend de la mise à jour du programme, et tout particulièrement de celle du fichier de définitions des virus et du moteur de recherche. Le composant Updater est intégré dans votre produit Avira pour l'exécution des mises à jour. Il garantit que votre produit Avira fonctionne toujours au niveau le plus récent et qu'il est en mesure de détecter les nouveaux virus apparaissant chaque jour. L'Updater met à jour les composants suivants :

- Fichier de définitions des virus :

  Le fichier de définitions des virus contient le modèle de détection des programmes malveillants, que votre produit Avira utilise lors de la recherche de virus et de logiciels malveillants, ainsi que lors de la réparation des objets infectés.

- Moteur de recherche :

  Le moteur de recherche contient les méthodes à l'aide desquelles votre produit Avira recherche des virus et logiciels malveillants.

- Fichiers de programme (mise à jour du produit) :

  Les paquets pour les mises à jour du produit offrent des fonctions supplémentaires pour les différents composants du programme.

Lors de l'exécution d'une mise à jour, on vérifie que le fichier de définitions des virus, le moteur de recherche et les fichiers de programme sont actuels, et ils sont mis à jour si nécessaire. Après une mise à jour du produit, il peut être nécessaire d'effectuer un redémarrage de votre ordinateur. S'il ne s'effectue qu'une mise à jour du fichier de définitions des virus et du moteur de recherche, il n'est pas nécessaire de redémarrer votre ordinateur.

Si un redémarrage est nécessaire après une mise à jour du produit, vous pouvez décider si vous souhaitez poursuivre la mise à jour ou si vous souhaitez recevoir un rappel ultérieur. Si vous décidez de poursuivre la mise à jour, vous devez tout de même déterminer le moment où l'ordinateur doit être redémarré.

Si vous désirez exécuter la mise à jour du produit à une date ultérieure, le fichier de définitions des virus et le moteur de recherche sont tout de même actualisés, mais pas les fichiers de programme.

Remarque
La mise à jour du produit n'est pas achevée tant que l'ordinateur n'a pas été redémarré.

Remarque
Pour des raisons de sécurité, l'Updater contrôle si le fichier hôte Windows de votre ordinateur a été modifié, si l'URL de mise à jour a par ex. été manipulée



par un logiciel malveillant, et redirige l'Updater vers des pages de téléchargement indésirables. Si le fichier hôte Windows a été manipulé, l'opération est visible dans le fichier rapport de l'Updater.

Une mise à jour est exécutée automatiquement dans l'intervalle suivant : 2 heures.

Dans le Control Center, sous **Planificateur**, vous pouvez configurer d'autres tâches de mise à jour qui seront exécutées par l'Updater aux intervalles indiqués. Vous avez aussi la possibilité de démarrer manuellement une mise à jour :

- Dans le Control Center : dans le menu **Mise à jour** et sous la rubrique **État**
- Via le menu contextuel de l'icône de la barre d'état

Vous pouvez obtenir des mises à jour à partir d'Internet, via un serveur Web du fabricant. Par défaut, la connexion réseau existante est utilisée comme connexion aux serveurs de téléchargement Avira. Vous pouvez adapter ce paramètre par défaut sous Configuration > Mise à jour.



7. FireWall

Avira Internet Security vous permet de surveiller et de réguler le trafic de données entrantes et sortantes en fonction des paramètres de votre ordinateur :

- Avira FireWall

Pour les systèmes d'exploitation jusqu'à Windows 7, Avira FireWall est compris dans votre Avira Internet Security.



8. Sauvegarde

Vous avez différentes possibilités de créer une sauvegarde de vos données :

Sauvegarde via l'outil de sauvegarde

À l'aide de l'outil de sauvegarde, vous pouvez sélectionner ou créer des profils de sauvegarde et lancer manuellement une sauvegarde pour un profil sélectionné .

Sauvegarde via une tâche de sauvegarde dans le planificateur

Le planificateur vous permet de créer des tâches de sauvegarde programmées ou commandées par événement. Le planificateur exécute automatiquement les tâches de sauvegarde. Ce procédé convient si vous souhaitez sauvegarder régulièrement certaines données .

9. Résolution des problèmes, astuces

Dans ce chapitre, vous trouverez des indications importantes pour résoudre des problèmes, ainsi que d'autres astuces pour utiliser votre produit Avira.

- voir chapitre Aide en cas de problème
- voir chapitre Commandes clavier
- voir chapitre Centre de sécurité Windows (pour Windows XP et Vista) ou Centre de maintenance Windows (à partir de Windows 7)

9.1 Aide en cas de problème

Vous trouverez ici des informations sur les causes et solutions de problèmes possibles.

- Le message d'erreur *Le fichier de licence ne s'ouvre pas* s'affiche.
- Le message d'erreur *L'établissement de la connexion a échoué lors du téléchargement du fichier...* apparaît lorsque vous essayez de démarrer une mise à jour.
- Les virus et logiciels malveillants ne peuvent pas être déplacés ou supprimés.
- L'icône de la barre d'état indique un état de désactivation.
- L'ordinateur devient très lent quand j'enregistre des données.
- Mon pare-feu signale la protection temps réel Avira et la protection e-mail Avira dès qu'elles sont actives
- La protection e-mail Avira ne fonctionne pas.
- Aucune connexion réseau n'est disponible dans les machines virtuelles, si l'Avira FireWall est installé sur le système d'exploitation hôte et le niveau de sécurité de l'Avira FireWall est réglé sur *Moyen* ou *Élevé*.
- La connexion Virtual Private Network (VPN) est bloquée si le niveau de sécurité de l'Avira FireWall est réglé sur *Moyen* ou *Élevé*.
- Un e-mail envoyé via une connexion TLS a été bloqué par la protection e-mail.
- Le chat Internet ne fonctionne pas : les messages du chat ne s'affichent pas.

Le message d'erreur *Le fichier de licence ne s'ouvre pas* s'affiche.

Cause : le fichier est codé.

- Pour activer la licence, il n'est pas nécessaire d'ouvrir le fichier mais il faut l'enregistrer dans le répertoire de programmes.



Le message d'erreur *L'établissement de la connexion a échoué lors du téléchargement du fichier...* apparaît lorsque vous essayez de démarrer une mise à jour.

Cause : votre connexion Internet est inactive. C'est pourquoi aucune connexion au serveur Web sur Internet ne peut être établie.

- Testez le fonctionnement d'autres services Internet comme WWW ou le courrier électronique. S'ils ne fonctionnent pas, restaurez la connexion Internet.

Cause : le serveur proxy n'est pas accessible.

- Contrôlez si les données de connexion au serveur proxy ont changé et adaptez votre configuration si nécessaire.

Cause : le fichier *update.exe* n'est pas intégralement autorisé par votre pare-feu personnel.

- Assurez-vous d'autoriser complètement le fichier *update.exe* auprès de votre pare-feu.

Sinon :

- Vérifiez dans la configuration (mode expert) sous Sécurité PC > Mise à jour.

Les virus et logiciels malveillants ne peuvent pas être déplacés ou supprimés.

Cause : le fichier a été chargé par Windows et se trouve à l'état activé.

- Actualisez votre produit Avira.
- Si vous utilisez le système d'exploitation Windows XP, désactivez la restauration du système.
- Démarrez l'ordinateur en mode sécurisé.
- Ouvrez la configuration de votre produit Avira (mode expert).
- Sélectionnez **Scanner > Recherche**, dans le champ *Fichier* sélectionnez l'option **Tous les fichiers** et confirmez la fenêtre avec **OK**.
- Démarrez une recherche sur tous les lecteurs locaux.
- Démarrez l'ordinateur en mode normal.
- Effectuez une recherche en mode normal.
- Si aucun autre virus ni logiciel malveillant n'est détecté, activez la restauration du système si elle est disponible et doit être utilisée.

L'icône de la barre d'état indique un état de désactivation.

Cause : la protection temps réel a été désactivée.

- Dans le Control Center, cliquez sur le point **État** et dans la zone *Sécurité PC*, activez la **Protection temps réel**.

- OU -

- Cliquez avec le bouton droit de la souris sur l'icône de la barre d'état. Le menu contextuel s'ouvre. Cliquez sur **Activer la protection temps réel**.

Cause : la protection temps réel est bloquée par un pare-feu.

- Dans la configuration de votre pare-feu, définissez une autorisation générale pour la protection temps réel Avira. La protection temps réel Avira fonctionne uniquement avec l'adresse 127.0.0.1 (localhost). Aucune connexion à Internet n'est établie. Il en va de même pour la protection e-mail Avira.

Sinon :

- Vérifiez le type de démarrage du service Protection temps réel Avira. Le cas échéant, activez le service : dans la barre de démarrage, sélectionnez **Démarrer > Panneau de configuration**. Lancez la fenêtre de configuration **Services** par double clic (sous Windows XP, vous trouvez l'applet Services dans le sous-dossier *Outils d'administration*). Recherchez l'entrée *Protection temps réel Avira*. Comme type de démarrage, vous devez sélectionner `Automatique` et comme statut `Démarré`. Le cas échéant, démarrez le service manuellement en sélectionnant la ligne correspondante et le bouton **Démarrer**. Si un message d'erreur s'affiche, contrôlez l'affichage de l'événement.

L'ordinateur devient très lent quand j'enregistre des données.

Cause : la protection temps réel Avira parcourt tous les fichiers que la sauvegarde des données traite lors du processus de sauvegarde.

- Dans la configuration (mode expert), sélectionnez **Protection temps réel > Recherche > Exceptions** et saisissez le nom du processus du logiciel de sauvegarde.

Mon pare-feu signale la protection temps réel Avira et la protection e-mail Avira, dès qu'elles sont activées.

Cause : la communication de la protection temps réel Avira et de la protection e-mail Avira s'effectue via le protocole Internet TCP/IP. Un pare-feu surveille toutes les connexions via ce protocole.

- Définissez une autorisation générale pour la protection temps réel et la protection e-mail Avira. La protection temps réel Avira fonctionne uniquement avec l'adresse 127.0.0.1 (localhost). Aucune connexion à Internet n'est établie. Il en va de même pour la protection e-mail Avira.

La protection e-mail Avira ne fonctionne pas.

✓ Contrôlez la fonctionnalité de la protection e-mail Avira à l'aide des checklists suivantes, si des problèmes se produisent avec la protection e-mail Avira.



Checklists

- ✓ Vérifiez si votre client de messagerie se connecte au serveur par Kerberos, APOP ou RPA. Ces méthodes d'authentification ne sont pas prises en charge actuellement.
- ✓ Contrôlez si votre client de messagerie se connecte au serveur par SSL (également souvent appelé TLS - Transport Layer Security). La protection e-mail Avira ne prend pas en charge SSL et arrête donc les connexions codées SSL. Si vous voulez utiliser les connexions codées SSL sans la protection e-mail Avira, vous devez utiliser pour la connexion un autre port que les ports surveillés par la protection e-mail. Vous pouvez configurer les ports surveillés par la protection e-mail dans la configuration sous **Protection e-mail > Recherche**.
- ✓ La protection e-mail Avira (service) est-elle active ? Le cas échéant, activez le service : dans la barre de démarrage, sélectionnez **Démarrer > Panneau de configuration**. Lancez la fenêtre de configuration **Services** par double clic (sous Windows XP, vous trouvez l'applet Services dans le sous-dossier *Outils d'administration*). Recherchez l'entrée *Protection e-mail Avira*. Comme type de démarrage, vous devez sélectionner `Automatique` et comme statut `Démarré`. Le cas échéant, démarrez le service manuellement en sélectionnant la ligne correspondante et le bouton **Démarrer**. Si un message d'erreur s'affiche, contrôlez l'*Affichage de l'événement*. Si cela ne résout pas le problème, désinstallez complètement le produit Avira via **Démarrer > Panneau de configuration > Programmes**, redémarrez l'ordinateur et réinstallez ensuite votre produit Avira.

Généralités

- Les connexions POP3 codées via SSL (Secure Sockets Layer) (souvent appelées TLS (Transport Layer Security)) ne peuvent pas être protégées actuellement et sont ignorées.
- L'authentification lors de la connexion au serveur de messagerie électronique est actuellement prise en charge uniquement via des mots de passe. « Kerberos » et « RPA » ne sont actuellement pas pris en charge.
- Votre produit Avira ne contrôle pas l'absence de virus et de programmes indésirables dans les e-mails lors de leur expédition.

> **Remarque**
> Nous vous recommandons d'effectuer régulièrement des mises à jour Microsoft pour combler d'éventuelles lacunes de sécurité.

Aucune connexion réseau n'est disponible dans les machines virtuelles, si l'Avira FireWall est installé sur le système d'exploitation hôte et le niveau de sécurité de l'Avira FireWall est réglé sur *Moyen* ou *Élevé*.

Si l'Avira FireWall est installé sur un ordinateur sur lequel une machine virtuelle est aussi installée (par ex. VMWare, Virtual PC, etc.), toutes les connexions réseau de la machine virtuelle sont bloquées si le niveau de sécurité de l'Avira FireWall est réglé sur *Moyen* ou *Élevé*. Si le niveau de sécurité est réglé sur *Bas*, les connexions réseau sont autorisées.



Cause : la machine virtuelle émule une carte réseau par logiciel. Par cette émulation, les paquets de données du système hôte sont englobés dans des paquets spéciaux (UDP) et redirigés vers le système hôte, via la passerelle externe. Dans l'Avira FireWall, à partir du niveau de sécurité *Moyen*, ils sont bloqués par les paquets venant de l'extérieur.

Pour contourner ce problème, procédez comme suit :

- Dans le Control Center, sélectionnez la rubrique *SÉCURITÉ INTERNET* **> FireWall**.
- Cliquez sur le lien **Configuration**.
- La fenêtre de dialogue *Configuration* s'affiche. Vous vous trouvez dans la rubrique de configuration *Règles d'applications*.
- Activez le **mode expert**.
- Sélectionnez la rubrique de configuration **Règles d'adaptation**.
- Cliquez sur **Ajouter**.
- Sous *Règle entrante*, sélectionnez **UDP**.
- Donnez un *nom* à la règle dans la zone **Nom de la règle**.
- Cliquez sur **OK**.
- Vérifiez si la règle obéit à un niveau de priorité supérieur à la règle **Refuser tous les paquets IP**.

> **Avertissement**
> Cette règle présente des dangers potentiels, car elle autorise tous les paquets UDP. Après l'utilisation de votre machine virtuelle, repassez au niveau de sécurité précédent.

La connexion Virtual Private Network (VPN) est bloquée si le niveau de sécurité de l'Avira FireWall est réglé sur *Moyen* ou *Élevé*.

Cause : par défaut, tous les paquets qui ne correspondent pas aux règles prédéfinies ne sont pas autorisés. Les paquets envoyés par le logiciel VPN sont filtrés par ces règles, car ils n'entrent dans aucune autre catégorie en raison de leur type (paquets GRE).

- Ajoutez, dans les **règles d'adaptation** de la configuration de l'Avira FireWall, la règle **Autoriser les connexions VPN**, afin d'autoriser tous les paquets VPN.

Un e-mail envoyé via une connexion TLS a été bloqué par la protection e-mail.

Cause : Transport Layer Security (TLS : protocole de cryptage pour la transmission de données par Internet) n'est actuellement pas pris en charge par la protection e-mail. Vous disposez des possibilités suivantes pour envoyer l'e-mail :

- Utilisez un autre port que le port 25 utilisé par SMTP. Vous contournerez ainsi la surveillance de la protection e-mail.

- Renoncez à utiliser la connexion cryptée TLS et désactivez la prise en charge TLS de votre client de messagerie.
- Désactivez (provisoirement) la surveillance des e-mails sortants par la protection e-mail dans la configuration sous **Protection e-mail > Recherche**.

Le chat Internet ne fonctionne pas : les messages du chat ne s'affichent pas.

Ce phénomène peut se produire dans les chats basés sur le protocole HTTP avec 'transfer-encoding: chunked'.

Cause : la protection Web contrôle d'abord intégralement l'absence de virus et de programmes indésirables sur les données envoyées avant de charger celles-ci dans le navigateur Internet. Lors du transfert de données avec 'transfer-encoding: chunked', la protection Web ne peut pas déterminer la longueur des messages ou la quantité de données.

- Indiquez l'URL du chat Internet comme exception dans la configuration (voir configuration : Protection Web > Recherche > Exceptions).

9.2 Commandes clavier

Les commandes clavier - aussi appelées raccourcis clavier - permettent de naviguer dans le programme, d'accéder à divers modules et de démarrer des actions rapidement.

Ci-après, vous trouverez un aperçu des commandes clavier disponibles. Le chapitre correspondant de l'Aide vous donne plus d'informations sur les fonctionnalités et la disponibilité de ces commandes.

9.2.1 Dans les boîtes de dialogue

Commande clavier	Description
Ctrl + Tab **Ctrl + PgDn**	Navigation dans le Control Center Passer à la rubrique suivante.
Ctrl + Maj + Tab **Ctrl + PgDn**	Navigation dans le Control Center Passer à la rubrique précédente.



←↑→↓	Navigation dans les rubriques de configuration Faites d'abord glisser la souris sur la rubrique de configuration que vous souhaitez consulter. Naviguer entre les options dans un champ de liste déroulante sélectionné ou entre les options dans un groupe d'options.
Tab	Passer à l'option suivante ou au groupe d'options suivant.
Maj + Tab	Passer à l'option précédente ou au groupe d'options précédent.
Touche espace	Activation et désactivation d'une case à cocher lorsque l'option active est une case à cocher.
Alt + lettre soulignée	Sélectionner une option ou exécuter une commande.
Alt + ↓ **F4**	Ouvrir le champ de liste déroulante sélectionné.
Échap	Fermer le champ de liste déroulante sélectionné. Annuler la commande et fermer la boîte de dialogue.
Touche Entrée	Exécuter la commande pour l'option active ou le bouton actif.

9.2.2 Dans l'Aide

Commande clavier	Description
Alt + touche espace	Afficher le menu système.
Alt + Tab	Naviguer entre l'Aide et les autres fenêtres ouvertes.
Alt + F4	Fermer l'Aide.
Maj + F10	Afficher les menus contextuels de l'Aide.

Ctrl + Tab	Passer à la rubrique suivante dans la fenêtre de navigation.
Ctrl + Maj + Tab	Passer à la rubrique précédente dans la fenêtre de navigation.
PgUp	Passer au thème situé au-dessus du thème actuel dans le sommaire, l'index ou la liste des résultats de recherche.
PgDn	Passer au thème situé en dessous du thème actuel dans le sommaire, l'index ou la liste des résultats de recherche.
PgUp **PgDn**	Parcourir un thème.

9.2.3 Dans le Control Center

Généralités

Commande clavier	Description
F1	Afficher l'Aide
Alt + F4	Fermer le Control Center
F5	Actualiser la vue
F8	Ouvrir la configuration
F9	Démarrer mise à jour

Rubrique **Scanner**

Commande clavier	Description
F2	Renommer le profil sélectionné
F3	Démarrer la recherche avec le profil choisi

F4	Créer un raccourci sur le Bureau pour le profil sélectionné
Ins	Créer un nouveau profil
Suppr	Supprimer le profil sélectionné

Rubrique **FireWall**

Commande clavier	Description
Entrée	Propriétés

Rubrique **Quarantaine**

Commande clavier	Description
F2	Contrôler à nouveau l'objet
F3	Restaurer l'objet
F4	Envoyer l'objet
F6	Restaurer l'objet à l'emplacement...
Entrée	Propriétés
Ins	Ajouter le fichier
Suppr	Supprimer l'objet

Rubrique **Planificateur**

Commande clavier	Description
F2	Modifier la tâche
Entrée	Propriétés
Ins	Ajouter une nouvelle tâche
Suppr	Supprimer la tâche

Rubrique **Rapports**

Commande clavier	Description
F3	Afficher le fichier rapport
F4	Imprimer le fichier rapport
Entrée	Afficher le rapport
Suppr	Supprimer le(s) rapport(s)

Rubrique **Événements**

Commande clavier	Description
F3	Exporter le(s) événement(s)
Entrée	Afficher l'événement
Suppr	Supprimer le(s) événement(s)

9.3 Centre de sécurité Windows

- de Windows XP Service Pack 2 à Windows Vista -

9.3.1 Généralités

Le Centre de sécurité Windows vérifie l'état d'un ordinateur concernant les aspects importants de la sécurité.

Si un problème est constaté sur l'un de ces points importants (par ex. un programme antivirus obsolète), le Centre de sécurité envoie un avertissement et émet des recommandations pour mieux protéger l'ordinateur.

9.3.2 Le Centre de sécurité Windows et votre produit Avira

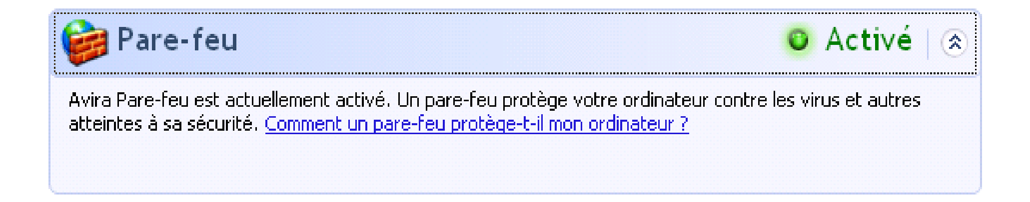
FireWall

Il est possible que vous receviez les informations suivantes du Centre de sécurité concernant le pare-feu :

- Pare-feu ACTIVÉ / Pare-feu en marche
- Pare-feu DÉSACTIVÉ / Pare-feu éteint

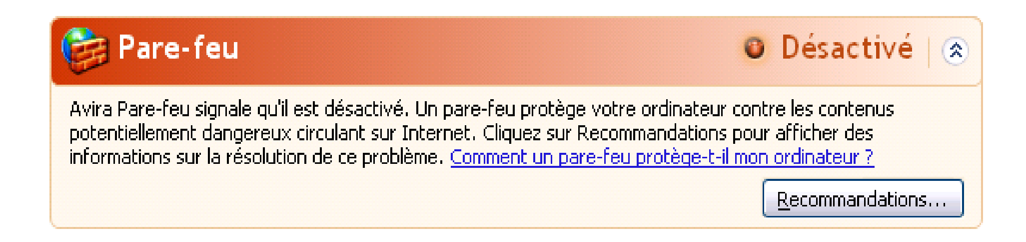
Pare-feu ACTIVÉ / Pare-feu en marche

Après l'installation de votre produit Avira et l'arrêt du pare-feu Windows, vous recevez le message suivant :



Pare-feu DÉSACTIVÉ / Pare-feu éteint

Vous recevez le message suivant dès que vous désactivez l'Avira FireWall :



Remarque
Vous pouvez activer et désactiver l'Avira FireWall via **État** dans le **Control Center**.



Avertissement
Si vous désactivez l'Avira FireWall, votre ordinateur n'est plus protégé des accès non autorisés via le réseau ou Internet.

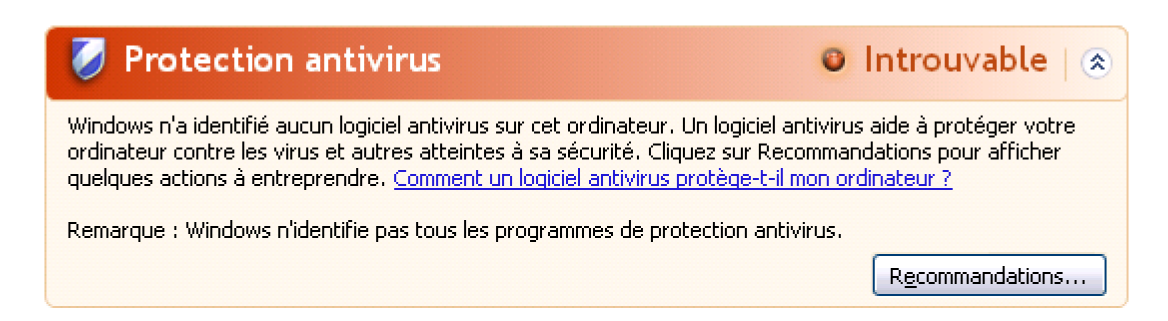
Logiciel antivirus / Protection contre les logiciels nuisibles

Vous pouvez recevoir les remarques suivantes du Centre de sécurité Windows, concernant votre protection antivirus.

- Protection antivirus NON TROUVÉE
- Protection antivirus EXPIRÉE
- Protection antivirus ACTIVÉE
- Protection antivirus DÉSACTIVÉE
- Protection antivirus NON SURVEILLÉE

Protection antivirus NON TROUVÉE

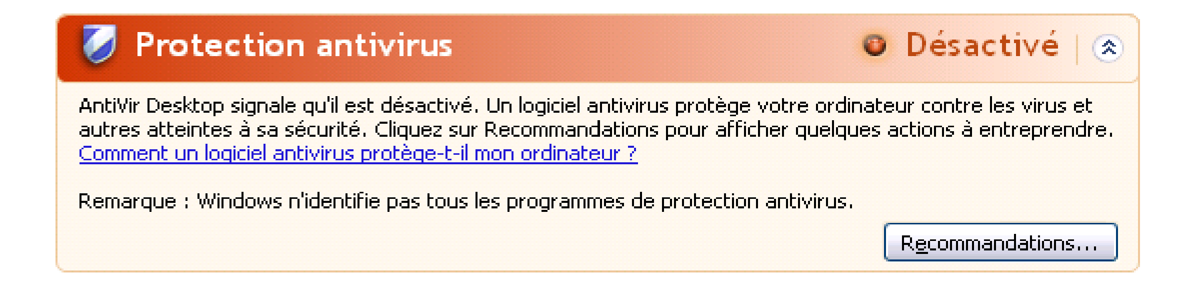
Cette notification du Centre de sécurité Windows apparaît si le Centre de sécurité Windows n'a trouvé aucun logiciel antivirus sur votre ordinateur.



Remarque
Installez votre produit Avira sur votre ordinateur pour le protéger des virus et autres programmes indésirables !

Protection antivirus EXPIRÉE

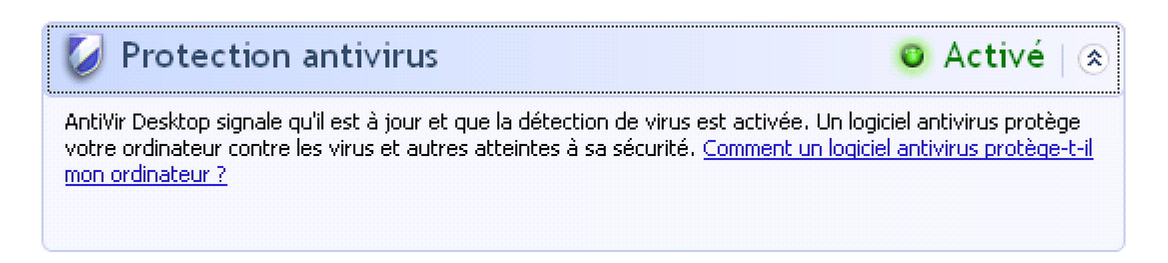
Si Windows XP Service Pack 2 ou Windows Vista est déjà installé sur votre ordinateur, puis que vous installez votre produit Avira, ou si vous installez Windows XP Service Pack 2 ou Windows Vista sur un système accueillant déjà votre produit Avira, vous recevez le message suivant :



Remarque
Pour que le Centre de sécurité Windows identifie votre produit Avira comme mis à jour, vous devez obligatoirement effectuer une mise à jour après l'installation. Vous actualisez votre système en exécutant une Mise à jour.

Protection antivirus ACTIVÉE

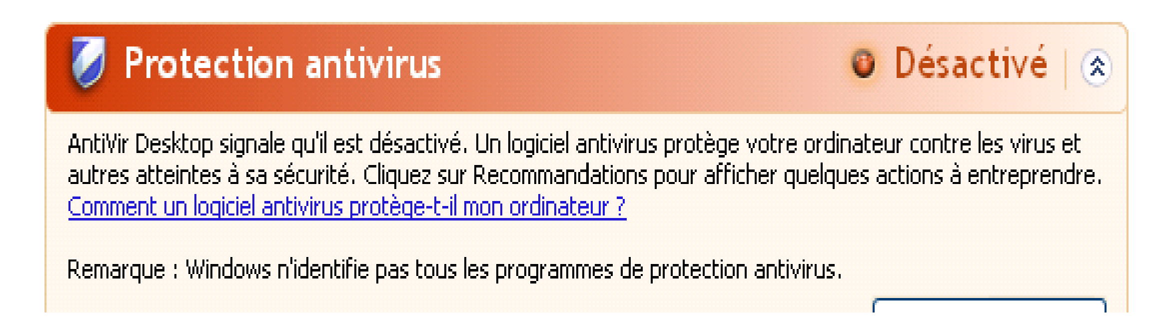
Après l'installation de votre produit Avira et après une mise à jour effectuée ensuite, vous recevez le message suivant :



Votre produit Avira est maintenant à jour et la protection temps réel Avira est activée.

Protection antivirus DÉSACTIVÉE

Vous recevez le message suivant si vous désactivez la protection temps réel Avira ou si vous arrêtez le service Protection temps réel.



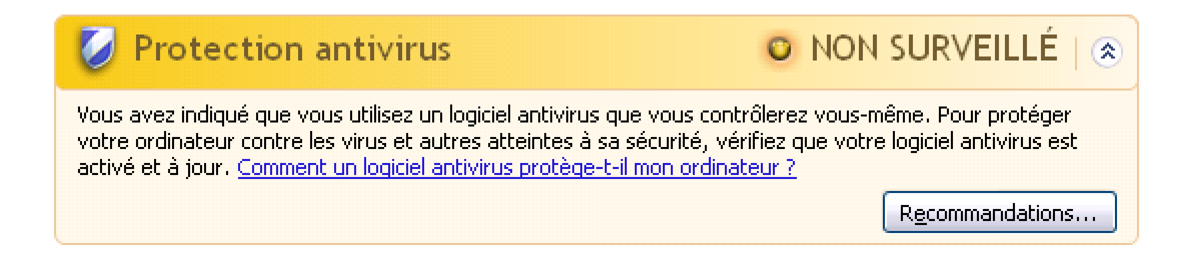
Remarque
Vous pouvez activer et désactiver la protection temps réel Avira sous la rubrique **État** du **Control Center**. Vous voyez en outre que la protection temps



réel Avira est activée lorsque le parapluie rouge est ouvert dans votre barre des tâches.

Protection antivirus NON SURVEILLÉE

Si vous recevez le message suivant du Centre de sécurité Windows, c'est que vous avez choisi de surveiller vous-même votre logiciel antivirus.



Remarque
Cette fonction n'est pas prise en charge par Windows Vista.

Remarque
Le centre de sécurité Windows est pris en charge par votre produit Avira. Vous pouvez activer cette option à tout moment via le bouton **Recommandations...**.

Remarque
Même si vous avez installé Windows XP Service Pack 2 ou Windows Vista, il vous faut toujours une protection antivirus. Bien que Windows surveille votre logiciel antivirus, il ne dispose d'aucune fonction antivirus. Aussi, sans protection antivirus supplémentaire, vous ne seriez donc pas protégé des virus et autres logiciels malveillants !

9.4 Centre de maintenance Windows

- Windows 7 et Windows 8 -

9.4.1 Généralités

Remarque :
à partir de Windows 7, le **Centre de sécurité Windows** a été renommé **Centre de maintenance Windows**. Dans cette section du programme, vous trouvez l'état de toutes les options de sécurité.

Le Centre de maintenance Windows vérifie l'état d'un ordinateur concernant les aspects importants de la sécurité. Vous pouvez accéder directement au Centre de maintenance en cliquant sur le petit drapeau de la barre des tâches ou sous **Panneau de configuration > Centre de maintenance**.

Si un problème est constaté sur l'un de ces points importants (par ex. un programme antivirus dépassé), le Centre de maintenance envoie un avertissement et émet des recommandations pour mieux protéger l'ordinateur. En d'autres termes, si tout fonctionne bien, vous ne recevez aucun message du Centre de maintenance. Cependant, il est possible de surveiller l'état de la sécurité de l'ordinateur dans le **Centre de maintenance** sous la rubrique **Sécurité**.
Vous avez également la possibilité de gérer et de sélectionner les logiciels que vous avez installés (par ex. *Afficher les programmes anti-espion installés*).

Vous pouvez désactiver les messages d'avertissement sous **Centre de maintenance > Modifier les paramètres**(par ex.*Désactiver les messages de sécurité pour la protection contre les logiciels espions et logiciels malveillants*).

9.4.2 Le Centre de maintenance Windows et votre produit Avira

Pare-feu du réseau

Il est possible que vous receviez les informations suivantes du Centre de maintenance concernant le pare-feu :

- Avira FireWall indique qu'il est activé
- Le pare-feu Windows et Avira FireWall indiquent qu'ils sont tous deux désactivés
- Pare-feu Windows est désactivé ou n'est pas configuré correctement

Avira FireWall indique qu'il est activé

Après l'installation de votre produit Avira et l'arrêt du pare-feu Windows, vous recevez le message suivant sous **Centre de maintenance > Sécurité > pare-feu réseau** : *Avira FireWall indique qu'il est activé*. Cela signifie que l'Avira FireWall est votre solution de pare-feu (faites bien la différence entre le pare-feu (produit Windows) et FireWall (produit Avira)).

Avertissement
Le **pare-feu Windows** n'est **pas** votre **Avira FireWall**. C'est pourquoi vous ne devez pas vous inquiéter si vous recevez des messages du genre : *Mettre à jour les paramètres du pare-feu* ou ***Le pare-feu Windows n'utilise pas les paramètres recommandés pour protéger votre ordinateur.*** **Votre produit Avira fonctionne sans problème et votre ordinateur est protégé**. Windows vous informe uniquement du fait que ses propres programmes sont désactivés.

Mettre à jour les paramètres du pare-feu

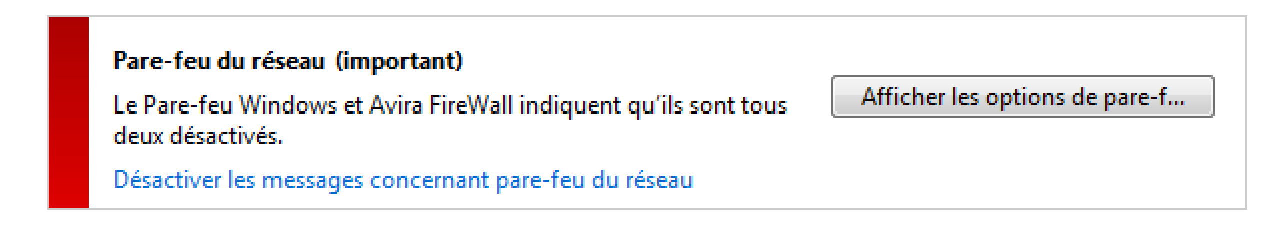
Le Pare-feu Windows n'utilise pas les paramètres recommandés pour protéger votre ordinateur.

Quels sont les paramètres recommandés ?

Utiliser les paramètres recommandés

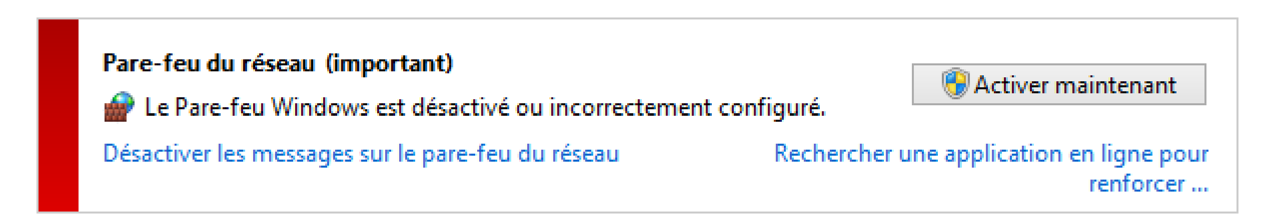
Le pare-feu Windows et Avira FireWall indiquent qu'ils sont tous deux désactivés

Vous recevez le message suivant dès que vous désactivez l'Avira FireWall :



Avertissement
Si vous désactivez l'**Avira FireWall**, votre ordinateur n'est plus protégé des accès non autorisés via le réseau ou Internet.

Pare-feu Windows est désactivé ou n'est pas configuré correctement



Cela signifie que ni **Pare-feu Windows**, ni l'**Avira FireWall** sont activés.

- **Sous Windows 7**

L'Avira Firewall est désactivé ou n'est pas configuré correctement. L'Avira FireWall doit être automatiquement reconnu par le Centre de maintenance. Veuillez redémarrer l'ordinateur. Si le problème persiste, réinstallez le produit Avira.

Protection antivirus

Vous pouvez recevoir les remarques suivantes du Centre de maintenance Windows, concernant votre protection antivirus :

- Avira Desktop indique être à jour et que la détection des virus est activée
- Avira Desktop indique qu'il est désactivé
- Avira Desktop indique qu'il est périmé
- Windows n'a pas trouvé de logiciel antivirus sur cet ordinateur



- Avira Desktop ne protège plus votre PC

Avira Desktop indique être à jour et que la détection des virus est activée

Après l'installation de votre produit Avira et après une mise à jour effectuée ensuite, vous ne recevez tout d'abord aucun message du Centre de maintenance Windows. Cependant, sous **Centre de maintenance > Sécurité**, vous pouvez trouver les indications suivantes : *« Avira Desktop » indique être à jour et que la détection de virus est activée*. Cela signifie que votre produit Avira est maintenant à jour et que la protection temps réel est activée.

Avira Desktop indique qu'il est désactivé

Vous recevez le message suivant si vous désactivez la protection temps réel Avira ou si vous arrêtez le service Protection temps réel.



Remarque
Vous pouvez activer ou désactiver la **protection temps réel Avira** sous la rubrique **État** de l'**Avira Control Center**. Vous voyez en outre que la **protection temps réel Avira** est activée lorsque le parapluie rouge est ouvert dans votre barre des tâches. Il est également possible d'activer les différents composants Avira en cliquant sur *Activer maintenant* du Centre de maintenance. Si vous obtenez un message où vous devez donner votre accord pour lancer le programme Avira, cliquez sur *Autoriser*, et la protection temps réel est activée.

Avira Desktop indique qu'il est périmé

Si vous venez d'installer Avira, ou si pour une raison quelconque le fichier de définitions des virus, le moteur de recherche ou les fichiers de programme de votre produit Avira n'ont pas été mis à jour automatiquement (par ex. si vous mettez à jour votre système d'exploitation, sur lequel vous avez déjà installé votre produit Avira, pour passer d'une ancienne version de Windows à une nouvelle), le message suivant s'affiche :

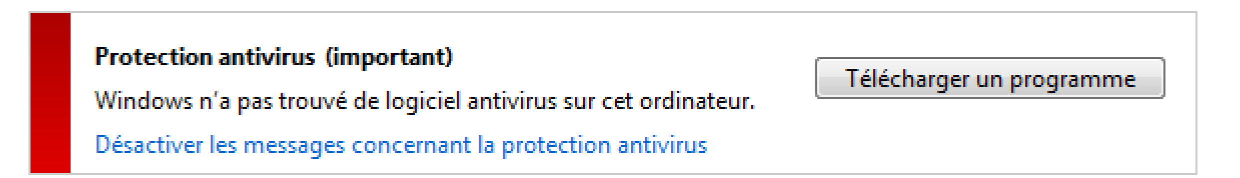




Remarque
Pour que le Centre de maintenance identifie votre produit Avira comme mis à jour, vous devez obligatoirement effectuer une mise à jour après l'installation. Vous actualisez votre système en exécutant une Mise à jour.

Windows n'a pas trouvé de logiciel antivirus sur cet ordinateur

Cette notification du Centre de maintenance Windows apparaît si le Centre de maintenance Windows n'a trouvé aucun logiciel antivirus sur votre ordinateur.



Remarque
Veuillez noter que cette option n'est pas disponible sous Windows 8. À partir de ce système d'exploitation, Windows Defender est la protection antivirus Microsoft par défaut.

Remarque
Installez votre produit Avira sur votre ordinateur pour le protéger des virus et autres programmes indésirables !

Avira Desktop ne protège plus votre PC

Cette information du Centre de maintenance Windows apparaît lorsque la licence de votre produit Avira a expiré.
Si vous cliquez sur le bouton **Entreprendre une action**, vous serez redirigé vers le site Web d'Avira, où vous pourrez obtenir une nouvelle licence.



Remarque
Veuillez noter que cette option n'est disponible que sous Windows 8.

Protection contre les logiciels espions et logiciels indésirables

Vous pouvez recevoir les remarques suivantes du Centre de maintenance Windows, concernant votre protection contre les logiciels espions et les logiciels indésirables :

- Avira Desktop indique qu'il est activé
- Windows Defender et Avira Desktop indiquent qu'ils sont tous deux désactivés
- Avira Desktop indique qu'il est périmé
- Windows Defender est périmé
- Windows Defender est désactivé

Avira Desktop indique qu'il est activé

Après l'installation de votre produit Avira et après une mise à jour effectuée ensuite, vous ne recevez tout d'abord aucun message du Centre de maintenance Windows. Cependant, sous **Centre de maintenance > Sécurité**, vous pouvez trouver les indications suivantes : *« Avira Desktop » indique qu'il est activé*. Cela signifie que votre produit Avira est à jour et que la protection temps réel est activée.

Windows Defender et Avira Desktop indiquent qu'ils sont tous deux désactivés

Vous recevez le message suivant si vous désactivez la protection temps réel Avira ou si vous arrêtez le service Protection temps réel.

Protection contre logiciels espions et programmes indésirables (important)

Windows Defender et Avira Desktop indiquent qu'ils sont tous deux désactivés.

Désactiver les messages concernant protection contre les logiciels espions

Afficher les programmes anti-e...

> **Remarque**
> Vous pouvez activer ou désactiver la **protection temps réel Avira** sous la rubrique **État** de l'**Avira Control Center**. Vous voyez en outre que la **protection temps réel Avira** est activée lorsque le parapluie rouge est ouvert dans votre barre des tâches. Il est également possible d'activer les différents composants Avira en cliquant sur *Activer maintenant* du Centre de maintenance. Si vous obtenez un message où vous devez donner votre accord pour lancer le programme Avira, cliquez sur *Autoriser*, et la protection temps réel est activée.



Avira Desktop indique qu'il est périmé

Si vous venez d'installer Avira, ou si pour une raison quelconque le fichier de définitions des virus, le moteur de recherche ou les fichiers de programme de votre produit Avira n'ont pas été mis à jour automatiquement (par ex. si vous mettez à jour votre système d'exploitation, sur lequel vous avez déjà installé votre produit Avira, pour passer d'une ancienne version de Windows à une nouvelle), le message suivant s'affiche :



Avira Desktop indique qu'il est périmé.

Mettre à jour

Désactiver les messages concernant protection contre les logiciels espions

Télécharger un autre programme anti-espion

Remarque
Pour que le Centre de maintenance identifie votre produit Avira comme mis à jour, vous devez obligatoirement effectuer une mise à jour après l'installation. Vous actualisez votre système en exécutant une Mise à jour.

Windows Defender est périmé

Le message suivant peut apparaître lorsque Windows Defender est activé. Cela peut indiquer que votre produit Avira n'a pas été correctement installé. Veuillez vérifier l'installation.

Protection contre logiciels espions et programmes indésirables (important)

Windows Defender est périmé.

Mettre à jour

Désactiver les messages concernant protection contre les logiciels espions

Télécharger un autre programme anti-espion

Remarque
Windows Defender est la solution prédéfinie contre les logiciels espions et pour la protection antivirus de Windows.

Windows Defender est désactivé

Vous recevez le message du Centre de maintenance Windows *Windows Defender est désactivé* lorsqu'aucun logiciel de protection contre les logiciels espions n'a été trouvé sur votre ordinateur. Windows Defender est un logiciel intégré par défaut dans le système d'exploitation pour identifier les logiciels espions. Si vous avez installé un autre logiciel antivirus sur votre ordinateur, cette application est désactivée.
Si votre produit Avira a été correctement installé, vous ne recevez plus ce message, car le Centre de maintenance identifie automatiquement Avira. Vérifiez si Avira fonctionne correctement.



Protection contre logiciels espions et programmes indésirables (important)

Windows Defender est désactivé.

Activer maintenant

Désactiver les messages concernant protection contre les logiciels espions

Télécharger un autre programme anti-espion

10. Virus et autres

Avira Internet Security identifie non seulement les virus et les logiciels malveillants, mais il peut également vous protéger contre d'autres dangers. Dans Ce chapitre, vous trouvez un aperçu des différents types de logiciels malveillants ainsi que des autres dangers encourus. Cette présentation décrit non seulement leur origine et leur comportement, mais également les mauvaises surprises qu'ils vous réservent.

Thèmes apparentés :

- Catégories de dangers
- Virus et autres logiciels malveillants

10.1 Catégories de dangers

Logiciels publicitaires

On appelle logiciel publicitaire un logiciel qui, en plus de sa fonctionnalité réelle, impose à l'utilisateur des bannières publicitaires ou fenêtres publicitaires intempestives. Ces affichages de publicités ne peuvent en général être désactivés et restent toujours visibles. Ici, les données de connexion permettent de tirer de nombreux renseignements sur le comportement d'utilisation et sont problématiques en matière de protection des données.

Votre produit Avira identifie les logiciels publicitaires. Si, dans la configuration, sous Catégories de dangers, l'option **Logiciels publicitaires** est activée, votre produit Avira vous avertit lorsqu'il détecte de tels logiciels.

Logiciels publicitaires/logiciels espions

Logiciel affichant de la publicité ou logiciel envoyant des informations personnelles de l'utilisateur à des tiers, le plus souvent sans son accord, ou à son issu, et qui est donc éventuellement indésirable.

Votre produit Avira identifie les logiciels publicitaires/espions. Si, dans la configuration, sous Catégories de dangers, l'option **Logiciels publicitaires/logiciels espions** est activée, votre produit Avira vous avertit lorsqu'il en détecte.

Application

L'appellation « Application » désigne une application dont l'utilisation peut être associée à un risque ou dont l'origine est douteuse.
Votre produit Avira détecte les applications (APPL). Si, dans la configuration, sous Catégories de dangers, l'option **Application** est activée, votre produit Avira vous avertit lorsqu'il détecte ce type de comportement.



Logiciels de commande Backdoor

Pour voler des données ou manipuler l'ordinateur, un programme de serveur backdoor passe par la « porte de derrière » sans que l'utilisateur ne le remarque. Via Internet ou le réseau, ce programme peut être commandé via un logiciel de commande backdoor (client) par des tiers.
Votre produit Avira détecte les logiciels de commande backdoor. Si, dans la configuration, sous Catégories de dangers, l'option **Logiciels de commande Backdoor** est activée, votre produit Avira vous avertit lorsqu'il détecte ce type de programme.

Fichiers à extensions déguisées

Fichiers exécutables qui déguisent leur extension de manière suspecte. Cette méthode de déguisement est souvent utilisée par les logiciels malveillants.
Votre produit Avira détecte les fichiers à extensions déguisées. Si, dans la configuration, sous Catégories de dangers, l'option **Fichiers à extensions déguisées** est activée, votre produit Avira vous avertit lorsqu'il en détecte.

Programme de numérotation payant

Certaines prestations de service sur Internet sont payantes. La facturation a lieu en Allemagne via les programmes de numérotation en 0190/0900 (en Autriche et en Suisse via des numéros en 09x0 ; en Allemagne le passage à des numéros en 09x0 aura lieu à moyen terme). Installés sur l'ordinateur, ces programmes, appelés dialers, assurent l'établissement de la connexion via un numéro surtaxé dont le prix peut être très variable.

La commercialisation de contenus en ligne via la facture téléphonique est légale et peut être avantageuse pour l'utilisateur. Les dialers sérieux affichent clairement leur utilisation consciente et réfléchie par le client. Ils ne s'installent sur l'ordinateur de l'utilisateur que si ce dernier a donné son accord, cet accord étant donné sur la base d'une présentation ou d'une incitation claires. L'établissement de la connexion via des programmes de numérotation sérieux s'affiche sans ambiguïté. En outre, les dialers sérieux indiquent clairement et avec précision les frais de connexion générés.

Malheureusement, il existe des dialers qui s'installent sur les ordinateurs de manière cachée et douteuse, voire à des fins frauduleuses. Ils remplacent par ex. la connexion de télétransmission standard de l'utilisateur Internet vers le FAI (fournisseur d'accès Internet) et appellent à chaque connexion un numéro en 0190/0900 surtaxé, parfois très cher. L'utilisateur ne remarque qu'après réception de la facture téléphonique suivante qu'un programme de numérotation indésirable en 0190/0900 a été utilisé sur son ordinateur à chaque connexion à Internet, avec pour conséquence des coûts très élevés.

Pour vous protéger des programmes de numérotation indésirables (dialers 0190/0900), nous vous conseillons de faire bloquer ce type de numéros directement auprès de votre opérateur téléphonique.

En général, votre produit Avira identifie les programmes de numérotation payants qu'il connaît.



Si, dans la configuration, sous Catégories de dangers, l'option **Programme de numérotation payant** est activée, votre produit Avira vous avertit lorsqu'il détecte un programme de ce type. Vous avez alors la possibilité de supprimer le programme de numérotation en 0190/0900. S'il s'agit d'un programme de numérotation souhaité, vous pouvez le déclarer comme fichier d'exclusion afin qu'il ne soit plus examiné à l'avenir.

Hameçonnage

L'hameçonnage, également connu sous le nom de « brand spoofing », est une forme raffinée de vol de données qui vise les clients ou clients potentiels des FAI, banques, services bancaires en lignes et autorités d'enregistrement.
Grâce à la transmission d'une adresse e-mail sur Internet, au remplissage de formulaires en ligne, à la participation à des groupes d'information ou par le biais de pages Web, il est possible que vos données soient volées par des « Internet crawling spiders » et utilisées sans votre accord pour une escroquerie ou d'autres forfaits.

Votre produit Avira détecte l'hameçonnage. Si, dans la configuration, sous Catégories de dangers, l'option **Hameçonnage** est activée, votre produit Avira vous avertit lorsqu'il détecte ce type de comportement.

Programmes portant atteinte à la vie privée

Logiciel qui compromet la sécurité de votre système, déclenche des activités de programmes non souhaitées, qui viole votre vie privée ou espionne votre comportement d'utilisateur et peut donc être indésirable.

Votre produit Avira détecte les logiciels de type « Security Privacy Risk ». Si, dans la configuration, sous Catégories de dangers, l'option **Programmes portant atteinte à la vie privée** est activée, votre programme Avira vous avertit lorsqu'il détecte des logiciels de ce type.

Programmes de blagues

Les programmes de blagues sont uniquement conçus pour effrayer ou pour amuser, sans être nuisibles ni se multiplier. Souvent, l'ordinateur joue une mélodie à l'ouverture du programme de blague ou affiche quelque chose d'inhabituel à l'écran. On peut citer à titre d'exemples la machine à laver dans le lecteur de disquettes (DRAIN.COM) et le mangeur d'écran (BUGSRES.COM).

Mais prudence ! Tous les signes des programmes de blagues peuvent aussi provenir d'un virus ou d'un cheval de Troie. Au mieux, vous en êtes quitte pour une belle frayeur, au pire la panique peut générer de véritables dégâts sur votre machine.

Votre produit Avira est capable de détecter les programmes de blagues grâce à l'élargissement de ses routines de recherche et d'identification, et le cas échéant, de les éliminer comme programmes indésirables. Si, dans la configuration, sous Catégories de dangers, l'option **Programmes de blagues** est activée, votre produit Avira vous avertit lorsqu'il détecte ce type de programmes.



Jeux

Les jeux sur ordinateur constituent une activité délassante, mais n'ont pas forcément leur place sur le lieu de travail (à part peut-être pour la pause déjeuner). Toutefois, dans les entreprises privées comme publiques, il n'est pas rare que les employés jouent. Internet permet de télécharger de nombreux jeux. Les jeux par e-mail aussi sont de plus en plus populaires : des simples échecs à la bataille navale, de nombreuses variantes circulent ; les jeux sont envoyés via les programmes de messagerie aux partenaires, qui répondent.

Des analyses ont montré que le temps de travail passé à jouer a atteint depuis longtemps des proportions économiques non négligeables. Il est d'autant plus compréhensible que de plus en plus d'entreprises décident de bannir les jeux des postes de travail.

Votre produit Avira identifie les jeux sur ordinateur. Si, dans la configuration, sous Catégories de dangers, l'option **Jeux** est activée, votre produit Avira vous avertit lorsqu'il détecte des jeux. Fin du jeu, au sens propre, car vous avez la possibilité de le supprimer.

Logiciels frauduleux

Également appelés « scareware » (logiciels destinés à effrayer) ou « rogueware » (logiciels fripouilles), il s'agit de logiciels frauduleux simulant des attaques virales et se proposant comme un logiciel antivirus professionnel. Le scareware est conçu pour inquiéter ou intimider l'utilisateur. Si la victime tombe dans le panneau et se pense menacée, elle se voit proposer contre paiement l'élimination du danger inexistant. Dans certains cas, la victime pensant être la cible d'une attaque est amenée à effectuer des manipulations qui elles, permettent alors une véritable attaque.

Si, dans la configuration, sous Catégories de dangers, l'option **Logiciels frauduleux** est activée, votre produit Avira vous avertit lorsqu'il détecte un scareware.

Logiciels de compression inhabituels

Fichiers compressés avec un programme de compression inhabituel et qui peuvent donc être considérés comme suspects.

Votre produit Avira détecte les logiciels de compression inhabituels. Si, dans la configuration, sous Catégories de dangers, l'option **Logiciels de compression inhabituels** est activée, votre produit Avira vous avertit lorsqu'il détecte l'un de ces programmes.

10.2 Virus et autres logiciels malveillants

Logiciels publicitaires

On appelle logiciel publicitaire un logiciel qui, en plus de sa fonctionnalité réelle, impose à l'utilisateur des bannières publicitaires ou fenêtres publicitaires intempestives. Ces affichages de publicités ne peuvent en général être désactivés et restent toujours visibles.

Ici, les données de connexion permettent de tirer de nombreux renseignements sur le comportement d'utilisation et sont problématiques en matière de protection des données.

Backdoors

Un backdoor (porte de derrière en français) peut accéder à un ordinateur en contournant sa protection.

Un programme fonctionnant de manière cachée offre à un agresseur des droits quasi illimités. À l'aide du backdoor, il est possible d'espionner les données personnelles de l'utilisateur. Mais ils servent surtout à installer des virus ou vers sur le système concerné.

Virus d'amorçage

Le secteur d'amorçage ou le secteur d'amorçage maître des disques durs est infecté de préférence avec des virus d'amorçage. Ils écrasent des informations importantes pour le démarrage du système. L'une des conséquences désagréables est la suivante : le système d'exploitation ne peut plus être chargé...

Bot-Net

Un Bot-Net est un réseau commandable à distance (sur Internet) constitué de PC qui se composent de bots communiquant entre eux. Ce contrôle est obtenu par des virus ou chevaux de Troie qui contaminent l'ordinateur puis attendent des instructions sans faire de dégâts sur l'ordinateur infecté. Ces réseaux peuvent être utilisés pour répandre des spams, des attaques DDoS, etc., parfois sans que les utilisateurs des PC concernés ne le remarquent. Le principal potentiel des Bot-Nets est de pouvoir atteindre une taille de plusieurs milliers d'ordinateurs dont la somme des bandes passantes dépasse largement la plupart des accès à Internet traditionnels.

Exploit

Un exploit (lacune de sécurité) est un programme informatique ou script qui exploite les faiblesses spécifiques ou dysfonctionnements d'un système d'exploitation ou d'un programme. Comme exemple d'exploit, on peut citer les attaques en provenance d'Internet à l'aide de paquets de données manipulés qui exploitent les faiblesses dans le logiciel de réseau. Dans ce cas, des programmes peuvent être infiltrés, permettant d'obtenir un accès plus important.

Canulars (hoaxes en anglais)

Depuis quelques années, les utilisateurs d'Internet et d'autres réseaux reçoivent des alertes aux virus qui se répandent par e-mail. Ces avertissements sont transmis par e-mail avec la consigne de les transférer au plus grand nombre de collègues et d'utilisateurs possible pour les prévenir du danger.



Pot de miel

Un pot de miel (honeypot en anglais) est un service installé dans un réseau (programme ou serveur). Il a la tâche de surveiller un réseau et de consigner les attaques. Ce service est inconnu de l'utilisateur légitime et n'est donc jamais sollicité. Quand un agresseur recherche alors les points faibles d'un réseau et sollicite les services proposés par un pot de miel, il est enregistré et une alarme se déclenche.

Macrovirus

Les macrovirus sont des petits programmes écrits dans le macrolangage d'une application (par ex. WordBasic sous WinWord 6.0) et peuvent se répandre normalement dans les documents de cette application seulement. On les appelle donc également des virus documents. Pour être activés, ils nécessitent le démarrage de l'application correspondante et l'exécution de l'une des macros contaminées. Contrairement aux virus « normaux », les macrovirus n'infectent donc pas les fichiers exécutables mais les documents de l'application hôte.

Pharming

Le pharming est une manipulation du fichier hôte des navigateurs Web pour dévier les requêtes sur des sites Web falsifiés. Il s'agit d'une variante de l'hameçonnage. Les escrocs utilisant le pharming entretiennent leurs propres grandes fermes de serveurs sur lesquelles des sites Web falsifiés sont archivés. Le pharming s'est établi comme terme générique pour plusieurs types d'attaques DNS. En cas de manipulation du fichier hôte, une manipulation ciblée du système est entreprise, à l'aide d'un cheval de Troie ou d'un virus. Par conséquent, seuls les sites Web contrefaits sont encore accessibles par le système, même quand l'adresse Web a été correctement saisie.

Hameçonnage

L'hameçonnage est la « pêche » aux données personnelles de l'utilisateur d'Internet. L'hameçonneur envoie à sa victime des courriers d'apparence officielle, comme par exemple des e-mails l'incitant à communiquer sans méfiance des informations confidentielles, surtout des identifiants et mots de passe ou PIN et TAN pour les opérations bancaires en ligne. Avec les données d'accès volées, l'hameçonneur peut prendre l'identité de sa victime et agir en son nom. Une chose est certaine : les banques et assurances ne demandent jamais d'envoyer les numéros de cartes de crédit, PIN, TAN ou autres données d'accès par e-mail, SMS ou téléphone.

Virus polymorphes

Les virus polymorphes sont de véritables maîtres du camouflage et du déguisement. Ils modifient leurs propres codes de programmation et sont donc particulièrement difficiles à identifier.

Virus programmes

Un virus informatique est un programme capable de se lier à d'autres programmes et de les infecter, une fois qu'il a été ouvert. Les virus se multiplient donc seuls, contrairement aux bombes logiques et aux chevaux de Troie. Contrairement à un ver, le virus nécessite toujours un programme tiers comme hôte, dans lequel il dépose son code virulent. Toutefois, le déroulement même du programme de l'hôte n'est normalement pas modifié.

Rootkits

Un rootkit est un ensemble d'outils logiciels furtifs qui s'installent après avoir infiltré un système informatique, pour masquer la connexion de l'envahisseur, cacher des processus et récupérer des données - en résumé : pour se rendre invisible. Il essaie d'actualiser les programmes d'espionnage déjà installés et de réinstaller les logiciels espions supprimés.

Virus de script et vers

Ces virus sont extrêmement simples à programmer et se répandent - quand les conditions techniques sont réunies - par e-mail dans le monde entier en quelques heures.

Les virus et vers de script utilisent l'un des langages de script, par ex. Javascript, VBScript etc., pour s'insérer dans de nouveaux scripts ou se répandre par l'activation de fonctions du système d'exploitation. La contamination a souvent lieu par e-mail ou lors de l'échange de fichiers (documents).

On appelle ver un programme qui se multiplie sans contaminer d'hôte. Les vers ne peuvent donc pas devenir partie intégrante d'autres processus programmes. Les vers constituent souvent la seule possibilité d'infiltrer des programmes nuisibles sur les systèmes équipés de mesures de sécurité très strictes.

Logiciels espions

Les logiciels espions sont des programmes qui envoient les données personnelles de l'utilisateur à son insu et sans son accord au fabricant du logiciel ou à un tiers. La plupart du temps, les programmes espions servent à analyser le comportement de navigation de l'utilisateur sur Internet et à afficher des bannières ou fenêtres publicitaires intempestives ciblées.

Chevaux de Troie

Les chevaux de Troie sont devenus fréquents ces derniers temps. C'est ainsi que l'on appelle les programmes qui semblent avoir une fonction spéciale mais dévoilent leur véritable finalité après leur démarrage et exécutent une autre fonction souvent néfaste. Les chevaux de Troie ne peuvent pas se multiplier seuls, ce qui les différencie des virus et vers. La plupart portent un nom intéressant (SEX.EXE ou STARTME.EXE) pour inciter l'utilisateur à exécuter le cheval de Troie. Ils sont actifs dès l'exécution et formatent par

exemple le disque dur. Les droppers qui inoculent des virus dans un système informatique constituent un type particulier de cheval de Troie.

Logiciels frauduleux

Également appelés « scareware » (logiciels destinés à effrayer) ou « rogueware » (logiciels fripouilles), il s'agit de logiciels frauduleux simulant des attaques virales et se proposant comme un logiciel antivirus professionnel. Le scareware est conçu pour inquiéter ou intimider l'utilisateur. Si la victime tombe dans le panneau et se pense menacée, elle se voit proposer contre paiement l'élimination du danger inexistant. Dans certains cas, la victime pensant être la cible d'une attaque est amenée à effectuer des manipulations qui elles, permettent alors une véritable attaque.

Zombie

Un PC zombie est un ordinateur infecté par des programmes malveillants et qui permet aux pirates informatiques d'utiliser l'ordinateur à distance dans un but criminel. Le PC infecté lance sur demande, par exemple, des attaques de type Denial-of-Service (DoS) ou envoie des spams et des e-mails d'hameçonnage.

11. Info et service

Dans ce chapitre, vous trouverez les informations nécessaires pour nous contacter.

- voir chapitre Adresse de contact
- voir chapitre Support technique
- voir chapitre Fichier suspect
- voir chapitre Signaler une fausse alerte
- voir chapitre Vos réactions pour plus de sécurité

11.1 Adresse de contact

Nous serons heureux de vous aider en cas de questions et de suggestions concernant la gamme de produits Avira. Vous trouverez nos adresses de contact dans le Control Center sous **Aide > À propos de Avira Internet Security**.

11.2 Support technique

Le support Avira est à vos côtés lorsqu'il s'agit de répondre à vos questions ou de résoudre un problème technique.

Sur notre site Web, vous obtiendrez toutes les informations nécessaires pour bénéficier de notre vaste service de support :
http://www.avira.com/fr/premium-suite-support

Pour nous permettre de vous aider rapidement et de manière fiable, préparez les informations suivantes :

- **Données de licence**. Vous les trouverez dans l'interface programme sous la rubrique **Aide > À propos de Avira Internet Security > Informations de licence**. Voir Informations de licence.
- **Informations de version**. Vous trouverez ces informations sous la rubrique **Aide > À propos de Avira Internet Security > Informations de version**. Voir Informations de version.
- **Version du système d'exploitation** et service packs éventuellement installés.
- **Packs logiciels installés**, par ex. logiciels antivirus d'autres fabricants.
- **Messages précis** du programme ou du fichier rapport.

11.3 Fichier suspect

Vous pouvez nous envoyer des fichiers suspects ou des virus qui ne peuvent pas encore être détectés ou supprimés par nos produits. Nous mettons plusieurs moyens à votre disposition.

- Sélectionnez le fichier dans le gestionnaire de quarantaines du Control Center puis, via le menu contextuel ou le bouton correspondant, sélectionnez le point **Envoyer fichier**.
- Envoyez le fichier souhaité sous forme compressée (WinZIP, PKZip, Arj, etc.) en pièce jointe par e-mail à l'adresse suivante :
  virus-premium-suite-fr@avira.com
  . Comme certaines passerelles de courrier électronique fonctionnent avec un logiciel antivirus, dotez le ou les fichier(s) d'un mot de passe (n'oubliez pas de nous communiquer ce mot de passe).
- Vous pouvez également nous envoyer le fichier suspect via notre site Web :
  http://www.avira.com/fr/sample-upload

11.4 Signaler une fausse alerte

Si vous pensez que votre produit Avira notifie un résultat positif dans un fichier très vraisemblablement « propre », envoyez ce fichier compressé (WinZIP, PKZIP, Arj, etc.) en pièce jointe par mail à l'adresse suivante :
virus-premium-suite-fr@avira.com

Comme certaines passerelles de courrier électronique fonctionnent avec un logiciel antivirus, dotez le ou les fichier(s) d'un mot de passe (n'oubliez pas de nous communiquer ce mot de passe).

11.5 Vos réactions pour plus de sécurité

Chez Avira, la sécurité de nos clients est la première de nos préoccupations. Pour cette raison, nous ne nous appuyons pas seulement sur notre propre équipe interne d'experts qui fait subir à chaque solution Avira et à chaque mise à jour des tests de qualité et de sécurité poussés avant publication. Nous attachons également la plus grande importance à vos remarques sur d'éventuelles faiblesses de sécurité et nous les traitons ouvertement.

Si vous pensez avoir trouvé un point de vulnérabilité dans la sécurité de l'un de nos produits, merci d'envoyer un e-mail à l'adresse suivante :

vulnerabilities-premium-suite-fr@avira.com

12. Référence : options de configuration

La référence de la configuration documente toutes les options de configuration disponibles.

12.1 Scanner

La rubrique **Scanner** de la configuration est en charge de la configuration de la recherche directe, c'est-à-dire de la recherche à la demande. (Options disponibles uniquement si le mode expert est activé.)

12.1.1 Recherche

Vous pouvez définir le comportement de base de la routine de recherche lors d'une recherche directe (Options disponibles uniquement si le mode expert est activé). Si vous choisissez certains répertoires à contrôler lors de la recherche directe, le scanner effectue le contrôle en fonction de la configuration :

- avec un niveau de recherche défini (priorité),
- plus les secteurs d'amorçage et la mémoire principale,
- tous les fichiers du répertoire, ou seulement certains.

Fichiers

Le scanner peut utiliser un filtre pour ne contrôler que les fichiers avec une extension particulière (type).

Tous les fichiers

Si cette option est activée, tous les fichiers sont parcourus à la recherche de virus et programmes indésirables, quels que soient leur contenu et leur extension. Le filtre n'est pas utilisé.

> **Remarque**
> Si l'option **Tous les fichiers** est activée, le bouton **Extensions de fichiers** ne peut pas être utilisé.

Sélection intelligente des fichiers

Si cette option est activée, la sélection des fichiers à contrôler est effectuée automatiquement par le programme. Cela signifie que votre programme Avira décide en fonction du contenu d'un fichier si celui-ci doit être contrôlé quant à l'absence de virus et programmes indésirables. Ce processus est un peu plus lent que l'option **Utiliser la liste des extensions de fichiers**, mais beaucoup plus sûr, car le contrôle

n'a pas lieu uniquement sur la base des extensions de fichiers. Ce paramètre est activé par défaut et recommandé.

> **Remarque**
> Si l'option **Sélection intelligente des fichiers** est activée, le bouton **Extensions de fichiers** ne peut pas être utilisé.

Utiliser la liste des extensions de fichiers

Si cette option est activée, seuls les fichiers dont l'extension a été présélectionnée sont contrôlés. Sont présélectionnés par défaut tous les types de fichiers pouvant contenir des virus et programmes indésirables. Cette liste peut être modifiée manuellement à l'aide du bouton « **Extensions de fichiers** ».

> **Remarque**
> Si cette option est activée et que vous avez supprimé toutes les entrées de la liste des extensions de fichiers, ceci est signalé avec le texte « *Aucune extension de fichiers* », sous le bouton **Extensions de fichiers**.

Extensions de fichiers

Ce bouton permet d'ouvrir une boîte de dialogue contenant toutes les extensions de fichiers examinées lors d'une recherche en mode « **Utiliser la liste des extensions de fichiers** ». Pour les extensions, des entrées sont indiquées par défaut, mais il est possible d'ajouter et de supprimer des entrées.

> **Remarque**
> Notez que la liste par défaut peut changer d'une version à l'autre.

Autres paramètres

Secteur d'amorçage des lecteurs

Si cette option est activée, le scanner contrôle les secteurs d'amorçage des lecteurs sélectionnés pour la recherche directe. Ce paramètre est activé par défaut.

Scanner les secteurs d'amorçage maître

Si cette option est activée, le scanner contrôle les secteurs d'amorçage maître du ou des disques durs utilisés dans le système.

Ignorer les fichiers hors ligne

Si cette option est activée, la recherche directe ignore complètement les fichiers hors ligne lors d'une recherche. Cela signifie que la présence de virus et programmes indésirables n'est pas contrôlée sur ces fichiers. Les fichiers hors ligne sont des fichiers qui ont été déplacés physiquement par un système de gestion hiérarchique de

la mémoire (HSMS), du disque dur vers une bande, par exemple. Ce paramètre est activé par défaut.

Contrôle d'intégrité de fichiers système

Si cette option est activée, les fichiers système Windows les plus importants sont soumis à un contrôle particulièrement sûr concernant d'éventuelles modifications opérées par des logiciels malveillants, et ce à chaque recherche directe. Si un fichier modifié est trouvé, celui-ci est signalé comme résultat positif suspect. Cette fonction utilise beaucoup de ressources de l'ordinateur. C'est pourquoi l'option est désactivée par défaut.

> **Remarque**
> Cette fonction n'est disponible qu'à partir de Windows Vista.

> **Remarque**
> Si vous utilisez des outils de fournisseurs tiers qui modifient les fichiers système et adaptent l'écran d'amorçage ou de démarrage à vos besoins, veuillez ne pas utiliser cette option. Voici quelques exemples de ces outils : Skinpacks, TuneUp Utilities ou Vista Customization.

Recherche optimisée

Si cette option est activée, la capacité du processeur est utilisée de façon optimale lors d'une recherche effectuée par le scanner. Pour des raisons liées à la performance, la consignation lors d'une recherche optimisée s'effectue au maximum à un niveau par défaut.

> **Remarque**
> L'option n'est disponible que sur les ordinateurs multiprocesseurs.

Suivre les liens symboliques

Si cette option est activée, le scanner suit, lors d'une recherche, tous les liens symboliques du profil de recherche ou du répertoire sélectionné pour contrôler l'absence de virus et de logiciels malveillants dans les fichiers liés.

> **Remarque**
> L'option n'inclut aucun lien de fichiers (shortcuts) mais se réfère exclusivement aux liens symboliques (créés avec mklink.exe) ou aux Junction Points (créés avec junction.exe) qui sont présents de manière transparente dans le système de fichiers.



Recherche de rootkits en début de contrôle

Si cette option est activée, le scanner vérifie au démarrage le répertoire système Windows à la recherche de rootkits actifs, au moyen d'un processus dit accéléré. Ce processus contrôle l'absence de rootkits sur votre ordinateur de manière moins détaillée que le profil de recherche « **Recherche de rootkits** », il est toutefois exécuté beaucoup plus rapidement. Cette option ne modifie que les paramètres des profils que vous avez personnellement créés.

> **Remarque**
> La recherche de rootkits n'est pas disponible sous Windows XP 64 bits .

Scanner le Registre

Si cette option est activée, le système recherche la présence de renvois à des logiciels dommageables dans le Registre. Cette option ne modifie que les paramètres des profils que vous avez personnellement créés.

Ignorer les fichiers et les chemins sur les lecteurs réseau

Si cette option est activée, les lecteurs réseau reliés à l'ordinateur sont exclus de la recherche directe. Cette option est recommandée quand les serveurs ou d'autres postes de travail sont eux-mêmes protégés par un logiciel antivirus. Cette option est désactivée par défaut.

Processus de contrôle

Autoriser l'arrêt

Si cette option est activée, la recherche de virus ou programmes indésirables peut être arrêtée à tout moment avec le bouton « **Arrêt** » dans la fenêtre « **Luke Filewalker** ». Si vous avez désactivé ce paramètre, le bouton **Arrêt** est grisé dans la fenêtre « **Luke Filewalker** ». L'arrêt prématurée d'une recherche n'est alors pas possible. Ce paramètre est activé par défaut.

Priorité du scanner

Le scanner distingue trois niveaux de priorité lors de la recherche directe. Cette distinction ne s'applique que si plusieurs processus fonctionnent en même temps sur l'ordinateur. Le choix influe sur la vitesse de la recherche.

basse

Le scanner reçoit du système d'exploitation du temps processeur uniquement si aucun autre processus ne nécessite de temps de calcul, c'est-à-dire que tant que le scanner fonctionne seul, la vitesse est maximale. Globalement, le travail avec les autres programmes est ainsi facilité : l'ordinateur réagit plus vite si d'autres programmes ont besoin de temps de calcul, pendant que le scanner continue de tourner en arrière-plan.

moyenne

Le scanner est exécuté avec le niveau de priorité normal. Tous les processus reçoivent du système d'exploitation le même temps processeur. Ce paramètre est activé par défaut et recommandé. Dans certaines conditions, le travail avec d'autres applications peut être entravé.

élevée

Le scanner obtient la priorité la plus élevée. Le travail en parallèle avec d'autres applications n'est quasiment plus possible. Toutefois, le scanner effectue sa recherche à la vitesse maximale.

Action si résultat positif

Vous pouvez définir les actions que le scanner doit exécuter quand un virus ou programme indésirable a été détecté. (Options disponibles uniquement si le mode expert est activé.)

Interactif

Si l'option est activée, les résultats positifs de la recherche du scanner sont signalés dans une fenêtre de dialogue. Lors de la recherche du scanner, vous recevez à l'issue de la recherche un message d'avertissement comportant une liste des fichiers contaminés qui ont été trouvés. Vous avez la possibilité de sélectionner une action à exécuter pour les différents fichiers concernés, via le menu contextuel. Vous pouvez exécuter les actions choisies pour tous les fichiers concernés ou quitter le scanner.

> **Remarque**
> L'action **Quarantaine** est présélectionnée par défaut dans la boîte de dialogue pour le traitement des virus. Vous pouvez sélectionner d'autres actions via un menu contextuel.

Automatique

Si l'option est activée, aucune boîte de dialogue permettant de sélectionner une action ne s'affiche en cas de détection d'un virus ou d'un programme indésirable. Le scanner réagit en fonction des paramètres que vous avez définis dans cette section.

Copier le fichier en quarantaine avant l'action

Si l'option est activée, le scanner génère une copie de sauvegarde (backup) avant d'exécuter l'action primaire ou secondaire souhaitée. La copie de sauvegarde est conservée en quarantaine où le fichier peut être restauré s'il a une valeur informative. En outre, vous pouvez envoyer la copie de sauvegarde à l'Avira Malware Research Center pour d'autres analyses.

Action primaire

L'action primaire est l'action exécutée lorsque le scanner trouve un virus ou un programme indésirable. Si l'option « **Réparer** » est sélectionnée, mais que la

réparation du fichier contaminé est impossible, l'action sélectionnée sous « **Action secondaire** » est exécutée.

> **Remarque**
> L'option **Action secondaire** ne peut être sélectionnée que si, sous **Action primaire**, le paramètre **Réparer** a été sélectionné.

Réparer

Si l'option est activée, le scanner répare automatiquement les fichiers contaminés. Si le scanner ne peut pas réparer un fichier contaminé, il exécute comme solution de rechange l'option choisie sous Action secondaire.

> **Remarque**
> Une réparation automatique est recommandée, mais cela signifie que le scanner modifie les fichiers sur l'ordinateur.

Renommer

Si l'option est activée, le scanner renomme le fichier. Un accès direct à ces fichiers (par un double clic par ex.) n'est alors plus possible. Les fichiers peuvent être réparés ultérieurement et à nouveau renommés.

Quarantaine

Si l'option est activée, le scanner déplace le fichier en quarantaine. Ces fichiers peuvent être réparés ultérieurement ou, si nécessaire, être envoyés à l'Avira Malware Research Center.

Supprimer

Si l'option est activée, le fichier est supprimé. Cette opération est nettement plus rapide que le processus **Écraser et supprimer** (voir ci-dessous).

Ignorer

Si l'option est activée, l'accès au fichier est autorisé et le fichier est conservé.

> **Avertissement**
> Le fichier contaminé reste actif sur votre ordinateur. D'importants dégâts peuvent être causés sur votre ordinateur.

Écraser et supprimer

Si l'option est activée, le scanner remplace le fichier par un modèle par défaut et le supprime ensuite. Il ne peut plus être restauré.

Action secondaire



L'option « **Action secondaire »** ne peut être sélectionnée que si le paramètre **Réparer** a été sélectionnée sous « **Action primaire »**. Cette option permet de décider ce qui doit advenir du fichier contaminé s'il n'est pas réparable.

Renommer

Si l'option est activée, le scanner renomme le fichier. Un accès direct à ces fichiers (par un double clic par ex.) n'est alors plus possible. Les fichiers peuvent être réparés ultérieurement et à nouveau renommés.

Quarantaine

Si l'option est activée, le scanner déplace le fichier en quarantaine. Ces fichiers peuvent être réparés ultérieurement ou, si nécessaire, être envoyés à l'Avira Malware Research Center.

Supprimer

Si l'option est activée, le fichier est supprimé. Cette opération est nettement plus rapide que le processus d'écrasement et de suppression.

Ignorer

Si l'option est activée, l'accès au fichier est autorisé et le fichier est conservé.

Avertissement
Le fichier contaminé reste actif sur votre ordinateur. D'importants dégâts peuvent être causés sur votre ordinateur.

Écraser et supprimer

Si l'option est activée, le scanner remplace le fichier par un modèle par défaut et le supprime ensuite. Il ne peut plus être restauré.

Remarque
Si vous avez sélectionné **Supprimer** ou **Écraser et supprimer** comme action primaire ou secondaire, tenez compte de ce qui suit : dans le cas de résultats heuristiques, les fichiers contaminés ne sont pas supprimés, mais déplacés en quarantaine.

Archives

Lors de la recherche dans les archives, le scanner peut utiliser une recherche récursive : les archives dans les archives sont décompressées et l'absence de virus et de programmes indésirables est contrôlée. Les fichiers sont contrôlés, décompressés et à nouveau contrôlés. (Options disponibles uniquement si le mode expert est activé.)

Contrôler les archives

Si cette option est activée, les archives sélectionnées dans la liste des archives sont contrôlées. Ce paramètre est activé par défaut.



Tous les types d'archives

Si cette option est activée, toutes les archives figurant dans la liste des archives sont sélectionnées et contrôlées.

Extensions intelligentes

Si cette option est activée, le scanner détecte si un fichier présente un format compressé (archive), même quand l'extension diffère des extensions habituelles, et contrôle l'archive. Pour cela, chaque fichier doit être ouvert, ce qui réduit la vitesse de recherche. Exemple : si une archive *.zip est dotée de l'extension *.xyz, le scanner décompresse également cette archive et la contrôle. Ce paramètre est activé par défaut.

> **Remarque**
> Seuls les types d'archives sélectionnés dans la liste des archives sont contrôlés.

Limiter la profondeur de récursivité

La décompression et le contrôle des archives à imbrication très profonde peut nécessiter beaucoup de temps de calcul et de ressources. Si cette option est activée, la profondeur de la recherche est limitée dans les archives multicompressées à un nombre défini sur les niveaux de paquets (profondeur de récursivité maximale). Vous économisez ainsi du temps et des ressources.

> **Remarque**
> Pour déterminer s'il y a un virus ou un programme indésirable au sein d'une archive, le scanner doit scanner celle-ci jusqu'au niveau de récursivité dans lequel le virus ou le programme indésirable se trouve.

Profondeur maximale de récursivité

Pour pouvoir saisir la profondeur de récursivité maximale, l'option **Limiter la profondeur de récursivité** doit être activée.
Vous pouvez soit saisir directement la profondeur de récursivité souhaitée, soit la modifier avec les touches fléchées à droite du champ de saisie. Les valeurs autorisées vont de 1 à 99. La valeur par défaut recommandée est de 20.

Valeurs par défaut

Le bouton restaure les valeurs prédéfinies pour la recherche dans les archives.

Liste des archives

Dans cette zone d'affichage, vous pouvez définir quelles archives le scanner doit contrôler. Pour cela, vous devez sélectionner les entrées correspondantes.

Exceptions

Objets de fichier à exclure par le scanner (Options disponibles uniquement si le mode expert est activé.)

La liste dans cette fenêtre contient les fichiers et chemins que le scanner doit ignorer lors de la recherche de virus et programmes indésirables.

Entrez ici aussi peu d'exceptions que possible et uniquement les fichiers qui ne doivent vraiment pas être contrôlés lors d'une recherche normale, pour quelque motif que ce soit. Nous recommandons dans tous les cas de contrôler l'absence de virus et de programmes indésirables sur ces fichiers, avant de les mettre dans la liste.

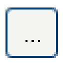
Remarque
Les entrées de la liste ne doivent pas dépasser 6 000 caractères au total.

Avertissement
Ces fichiers sont ignorés lors de la recherche.

Remarque
Les fichiers inscrits dans cette liste sont mentionnés dans le fichier rapport. Contrôlez de temps en temps le fichier rapport concernant ces fichiers non contrôlés car la raison pour laquelle vous aviez exclu un fichier n'existe peut-être plus. Dans ce cas, supprimez le nom de ce fichier de la liste.

Champ de saisie

Entrez dans ce champ le nom de l'objet de fichier qui doit être ignoré par la recherche directe. Aucun objet de fichier n'est indiqué par défaut.



Ce bouton ouvre une fenêtre dans laquelle vous pouvez sélectionner le fichier ou le chemin souhaité.
Si vous avez saisi un nom de fichier avec le chemin intégral, seul ce fichier n'est pas contrôlé. Si vous avez saisi un nom de fichier sans chemin, tout fichier portant ce nom (quel que soit le chemin ou le lecteur) ne sera pas contrôlé.

Ajouter

Ce bouton vous permet de reprendre dans la fenêtre d'affichage l'objet de fichier entré dans le champ de saisie.



Supprimer

Le bouton supprime une entrée sélectionnée de la liste. Ce bouton n'est pas actif si aucune entrée n'est sélectionnée.

Heuristique

Cette rubrique de configuration contient les paramètres pour l'heuristique du moteur de recherche. (Options disponibles uniquement si le mode expert est activé.)

Les produits Avira contiennent des heuristiques très performantes qui permettent de détecter dynamiquement des logiciels malveillants inconnus, c'est-à-dire avant même qu'une signature de virus spéciale n'ait été créée contre le parasite et qu'une mise à jour de protection antivirus correspondante n'ait été envoyée. La détection des virus s'effectue par une analyse complexe et un examen du code en cause, à la recherche de fonctions typiques des logiciels malveillants. Si le code examiné présente ces caractéristiques, il est signalé comme suspect. Cela ne signifie pas obligatoirement que le code est un logiciel malveillant ; des messages erronés peuvent aussi survenir. C'est l'utilisateur qui doit décider comment traiter le code, par ex. sur la base de ses connaissances pour savoir si la source contenant le code signalé est digne de confiance.

Heuristique de macrovirus

Heuristique de macrovirus

Votre produit Avira contient une heuristique de macrovirus très performante. Si l'option est activée, toutes les macros du document contaminé sont supprimées si une réparation est possible ; les documents suspects peuvent aussi être seulement signalés, c'est-à-dire que vous recevez un avertissement. Ce paramètre est activé par défaut et recommandé.

Advanced Heuristic Analysis and Detection (AHeAD)

Activer AHeAD

Votre programme Avira contient une heuristique très performante grâce à la technologie Avira AHeAD, lui permettant de détecter aussi les (nouveaux) logiciels malveillants inconnus. Si l'option est activée, vous pouvez régler ici la sensibilité de cette heuristique. Ce paramètre est activé par défaut.

Niveau de détection bas

Si l'option est activée, moins de logiciels malveillants inconnus sont détectés, le risque de détections erronées est faible dans ce cas.

Niveau de détection moyen

Si l'option est activée, une protection équilibrée est assurée avec peu de messages d'erreurs. Ce paramètre est activé par défaut si vous avez choisi l'utilisation de cette heuristique.



Niveau de détection élevé

Si l'option est activée, nettement plus de logiciels malveillants inconnus sont détectés, sachant qu'il faut toutefois s'attendre à des messages erronés.

12.1.2 Rapport

Le scanner dispose d'une fonction de consignation étendue. Vous obtenez ainsi des informations précises sur les résultats d'une recherche directe. Le fichier rapport contient toutes les données du système, ainsi que les avertissements et messages de la recherche directe. (Options disponibles uniquement si le mode expert est activé.)

> **Remarque**
> Pour vous permettre de savoir quelles actions le scanner a effectuées lors de la détection de virus ou de programmes indésirables, un fichier rapport doit systématiquement être généré.

Consignation

Désactivée

Si cette option est activée, le scanner ne consigne pas les actions et résultats de la recherche directe.

Par défaut

Si cette option est activée, le scanner consigne les noms des fichiers contaminés en indiquant leur chemin. En outre, la configuration de la recherche actuelle, les informations sur la version et sur le détenteur de la licence sont inscrites dans le fichier rapport.

Étendue

Si cette option est activée, le scanner consigne les avertissements et remarques en plus des informations standard. Le fichier rapport mentionne un suffixe « (Cloud) » pour identifier les avertissements de la protection Cloud.

Intégrale

Si cette option est activée, le scanner consigne également tous les fichiers contrôlés. En outre, tous les fichiers contaminés, ainsi que les avertissements et remarques sont repris dans le fichier rapport.

> **Remarque**
> Si vous devez nous envoyer un fichier rapport (pour la recherche d'erreur), merci de le générer dans ce mode.

12.2 Protection temps réel

La rubrique Protection temps réel de la configuration permet la configuration de la recherche en temps réel. (Options disponibles uniquement si le mode expert est activé.)

12.2.1 Recherche

En règle générale, vous voudrez surveiller votre système en continu. Pour ce faire, utilisez la protection temps réel (recherche en temps réel = On-Access Scanner). Cette protection vous permet de faire contrôler « à la volée » tous les fichiers copiés ou ouverts sur l'ordinateur à la recherche de virus et de programmes indésirables. (Option disponible uniquement si le mode expert est activé.)

Fichiers

La protection temps réel peut utiliser un filtre pour ne contrôler que les fichiers avec une certaine extension (type).

Tous les fichiers

Si cette option est activée, tous les fichiers sont parcourus à la recherche de virus et programmes indésirables, quels que soient leur contenu et leur extension.

> **Remarque**
> Si l'option **Tous les fichiers** est activée, le bouton **Extensions de fichiers** ne peut pas être utilisé.

Sélection intelligente des fichiers

Si cette option est activée, la sélection des fichiers à contrôler est effectuée automatiquement par le programme. Cela signifie que le programme décide en fonction du contenu d'un fichier si celui-ci doit être contrôlé quant à l'absence de virus et programmes indésirables. Ce processus est un peu plus lent que l'option **Utiliser la liste des extensions de fichiers**, mais beaucoup plus sûr, car le contrôle n'a pas lieu uniquement sur la base des extensions de fichiers.

> **Remarque**
> Si l'option **Sélection intelligente des fichiers** est activée, le bouton **Extensions de fichiers** ne peut pas être utilisé.

Utiliser la liste des extensions de fichiers

Si cette option est activée, seuls les fichiers dont l'extension a été présélectionnée sont contrôlés. Sont présélectionnés par défaut tous les types de fichiers pouvant contenir des virus et programmes indésirables. Cette liste peut être modifiée



manuellement à l'aide du bouton « **Extension de fichiers** ». Ce paramètre est activé par défaut et recommandé.

> **Remarque**
> Si cette option est activée et que vous avez supprimé toutes les entrées de la liste des extensions de fichiers, ceci est signalé avec le texte « *Aucune extension de fichiers* », sous le bouton **Extensions de fichiers**.

Extensions de fichiers

Ce bouton permet d'ouvrir une boîte de dialogue contenant toutes les extensions de fichiers examinées lors d'une recherche en mode « **Utiliser la liste des extensions de fichiers** ». Pour les extensions, des entrées sont indiquées par défaut, mais il est possible d'ajouter et de supprimer des entrées.

> **Remarque**
> Notez que la liste des extensions de fichiers peut changer d'une version à l'autre.

Mode de recherche

Définissez ici le moment où le contrôle d'un fichier doit avoir lieu.

Contrôler pendant la lecture

Si cette option est activée, la protection temps réel contrôle les fichiers avant qu'ils ne soient lus ou exécutés par une application ou le système d'exploitation.

Contrôler pendant l'écriture

Si cette option est activée, la protection temps réel contrôle un fichier lors de l'écriture. Ce n'est qu'après cette opération que vous pouvez accéder à nouveau au fichier.

Contrôler pendant la lecture et l'écriture

Si cette option est activée, la protection temps réel contrôle les fichiers avant l'ouverture, la lecture et l'exécution, et après l'écriture. Ce paramètre est activé par défaut et recommandé.

Lecteurs

Surveiller les lecteurs réseau

Si cette option est activée, les fichiers se trouvant sur les lecteurs réseau (lecteurs mappés), comme les volumes de serveur, les lecteurs clients, etc., sont surveillés.



Remarque
Pour ne pas trop restreindre les performances de votre ordinateur, activez l'option **Surveiller les lecteurs réseau** uniquement dans des cas exceptionnels.

Avertissement
Si l'option est désactivée, les lecteurs réseau ne sont **pas** surveillés. Vous n'êtes plus protégé des virus et programmes indésirables.

Remarque
Quand des fichiers sont exécutés sur des lecteurs réseau, ceux-ci sont contrôlés par la protection temps réel, indépendamment du réglage de l'option **Surveiller les lecteurs réseau**. Dans certains cas, les fichiers se trouvant sur des lecteurs réseau sont contrôlés à leur ouverture, bien que l'option **Surveiller les lecteurs réseau** soit désactivée. La raison : l'accès à ces fichiers s'effectue avec le droit « Exécuter le fichier ». Si vous souhaitez exclure ces fichiers, ou bien aussi des fichiers exécutés sur les lecteurs réseau, de la surveillance opérée par la protection temps réel, veuillez inscrire les fichiers dans la liste des objets de fichiers à exclure (voir : Exceptions).

Activer la gestion d'antémémoire

Si cette option est activée, les fichiers surveillés sur les lecteurs réseau sont mis à disposition dans la gestion d'antémémoire de la protection temps réel. La surveillance des lecteurs réseau sans fonction de gestion d'antémémoire offre plus de sécurité mais est moins performante que la surveillance de lecteurs réseau avec la fonction de gestion d'antémémoire.

Archives

Contrôler les archives

Si l'option est activée, les archives sont contrôlées. Les fichiers compressés sont contrôlés, décompressés et à nouveau contrôlés. Cette option est désactivée par défaut. La recherche dans les archives est limitée par le biais de la profondeur de récursivité, du nombre de fichiers à analyser et de la taille des archives. Vous pouvez régler la profondeur maximale de récursivité, le nombre de fichiers à contrôler et la taille maximale des archives.

Remarque
Cette option est désactivée par défaut car le processus utilise beaucoup de ressources de l'ordinateur. Généralement, il est conseillé de contrôler les archives avec la recherche directe.



Prof. de récursivité max.

Lors de la recherche dans les archives, la protection temps réel peut utiliser une recherche récursive : les archives dans les archives sont décompressées et l'absence de virus et de programmes indésirables est contrôlée. Vous pouvez définir la profondeur de récursivité. La valeur par défaut pour la profondeur de récursivité, qui est de 1, est conseillée : tous les fichiers se trouvant directement dans l'archive principale sont contrôlés.

Nombre max. de fich.

Lors de la recherche dans les archives, celle-ci est limitée à un nombre maximal de fichiers dans l'archive. La valeur par défaut pour le nombre maximal de fichiers à contrôler est de 10 et est recommandée.

Taille max. (Ko)

Lors de la recherche dans les archives, celle-ci est limitée à une taille maximale d'archive à décompresser. La valeur par défaut de 1 000 Ko est recommandée.

Action si résultat positif

Vous pouvez établir des actions que la protection temps réel doit exécuter quand un virus ou programme indésirable a été détecté. (Options disponibles uniquement si le mode expert est activé.)

Interactif

Si l'option est activée, une notification est affichée sur le Bureau en cas de résultat positif de la protection temps réel. Vous avez la possibilité de supprimer le logiciel malveillant trouvé ou d'appeler d'autres actions possibles pour le traitement du virus via le bouton « **Détails** ». Les actions sont affichées dans une boîte de dialogue. Cette option est activée par défaut.

Réparer

La protection temps réel répare le fichier contaminé si c'est possible.

Renommer

La protection temps réel renomme le fichier. Un accès direct à ces fichiers (par un double clic par ex.) n'est alors plus possible. Le fichier peut être réparé ultérieurement et à nouveau renommé.

Quarantaine

La protection temps réel déplace le fichier en quarantaine. Le fichier peut être restauré depuis le gestionnaire de quarantaines s'il a une valeur informative ou, si nécessaire, être envoyé à l'Avira Malware Research Center. Selon le fichier, d'autres possibilités de sélection sont disponibles dans le gestionnaire de quarantaines (voir Gestionnaire de quarantaines).

Supprimer

Le fichier est supprimé. Cette opération est nettement plus rapide que le processus **Écraser et supprimer** (voir ci-dessous).



Ignorer

L'accès au fichier est autorisé et le fichier est conservé.

Écraser et supprimer

La protection temps réel remplace le fichier par un modèle par défaut et le supprime ensuite. Il ne peut plus être restauré.

Avertissement
Si la protection temps réel est réglée sur **Contrôler pendant l'écriture**, le fichier contaminé n'est pas créé.

Par défaut

Ce bouton vous permet de sélectionner l'action activée par défaut dans la boîte de dialogue en cas de détection d'un virus. Sélectionnez l'action qui doit être activée par défaut et cliquez sur le bouton **« Par défaut »**.

Remarque
L'action **Réparer** ne peut pas être sélectionnée comme action par défaut.

Vous trouverez de plus amples informations ici.

Automatique

Si l'option est activée, aucune boîte de dialogue permettant de sélectionner une action ne s'affiche en cas de détection d'un virus ou d'un programme indésirable. La protection temps réel réagit en fonction des paramètres que vous avez définis dans cette section.

Copier le fichier en quarantaine avant l'action

Si l'option est activée, la protection temps réel génère une copie de sauvegarde (backup) avant d'exécuter l'action primaire ou secondaire souhaitée. La copie de sauvegarde est conservée en quarantaine. Elle peut être restaurée à tout moment par le gestionnaire de quarantaines si elle a une valeur informative. En outre, vous pouvez envoyer la copie de sauvegarde à l'Avira Malware Research Center. En fonction de l'objet, d'autres possibilités de sélection sont disponibles dans le gestionnaire de quarantaines (voir Gestionnaire de quarantaines).

Action primaire

L'action primaire est l'action effectuée lorsque la protection temps réel trouve un virus ou un programme indésirable. Si l'option « **Réparer** » est sélectionnée, mais que la réparation du fichier contaminé est impossible, l'action sélectionnée sous « **Action secondaire** » est exécutée.

> **Remarque**
> L'option **Action secondaire** ne peut être sélectionnée que si, sous **Action primaire**, le paramètre **Réparer** a été sélectionné.

Réparer

Si l'option est activée, la protection temps réel répare automatiquement les fichiers contaminés. Si la protection temps réel ne peut pas réparer un fichier contaminé, elle exécute comme solution de rechange l'option choisie sous **Action secondaire**.

> **Remarque**
> Une réparation automatique est recommandée, mais cela signifie que la protection temps réel modifie les fichiers sur l'ordinateur.

Renommer

Si l'option est activée, la protection temps réel renomme le fichier. Un accès direct à ces fichiers (par un double clic par ex.) n'est alors plus possible. Les fichiers peuvent être réparés ultérieurement et à nouveau renommés.

Quarantaine

Si l'option est activée, la protection temps réel déplace le fichier dans un répertoire de quarantaine. Les fichiers de ce répertoire peuvent être réparés ultérieurement ou, si nécessaire, être envoyés à l'Avira Malware Research Center.

Supprimer

Si l'option est activée, le fichier est supprimé. Cette opération est nettement plus rapide que le processus d'écrasement et de suppression.

Ignorer

Si l'option est activée, l'accès au fichier est autorisé et le fichier est conservé.

> **Avertissement**
> Le fichier contaminé reste actif sur votre ordinateur. D'importants dégâts peuvent être causés sur votre ordinateur.

Écraser et supprimer

Si l'option est activée, la protection temps réel remplace le fichier par un modèle par défaut et le supprime ensuite. Il ne peut plus être restauré.

Refuser l'accès

Si l'option est activée, la protection temps réel inscrit le résultat positif dans le fichier rapport uniquement si la fonction de rapport est activée. En outre, la protection temps réel inscrit une entrée dans le protocole d'événements, si cette option est activée.

Avertissement
Si la protection temps réel est réglée sur **Contrôler pendant l'écriture**, le fichier contaminé n'est pas créé.

Action secondaire

L'option « **Action secondaire** » ne peut être sélectionnée que si l'option « **Réparer** » a été sélectionnée sous « **Action primaire** ». Cette option permet de décider ce qui doit advenir du fichier contaminé s'il n'est pas réparable.

Renommer

Si l'option est activée, la protection temps réel renomme le fichier. Un accès direct à ces fichiers (par un double clic par ex.) n'est alors plus possible. Les fichiers peuvent être réparés ultérieurement et à nouveau renommés.

Quarantaine

Si l'option est activée, la protection temps réel déplace le fichier en quarantaine. Les fichiers peuvent être réparés ultérieurement ou, si nécessaire, être envoyés à l'Avira Malware Research Center.

Supprimer

Si l'option est activée, le fichier est supprimé. Cette opération est nettement plus rapide que le processus d'écrasement et de suppression.

Ignorer

Si l'option est activée, l'accès au fichier est autorisé et le fichier est conservé.

Avertissement
Le fichier contaminé reste actif sur votre ordinateur. D'importants dégâts peuvent être causés sur votre ordinateur.

Écraser et supprimer

Si l'option est activée, la protection temps réel remplace le fichier par un modèle par défaut et le supprime ensuite. Il ne peut plus être restauré.

Refuser l'accès

Si l'option est activée, le fichier contaminé n'est pas créé. La protection temps réel inscrit le résultat positif dans le fichier rapport uniquement si la fonction de rapport est activée. En outre, la protection temps réel inscrit une entrée dans le protocole d'événements, si cette option est activée.

Remarque
Si vous avez sélectionné **Supprimer** ou **Écraser et supprimer** comme action primaire ou secondaire, tenez compte de ce qui suit : dans le cas de résultats

heuristiques, les fichiers contaminés ne sont pas supprimés, mais déplacés en quarantaine.

Autres actions

Utiliser le rapport d'événement

Si cette option est activée, une entrée est inscrite dans le rapport d'événement Windows à chaque résultat positif. Les événements peuvent être consultés dans l'affichage des événements Windows. Ce paramètre est activé par défaut. (Options disponibles uniquement si le mode expert est activé.)

Exceptions

Ces options vous permettent de configurer des objets d'exclusion pour la protection temps réel (recherche en temps réel). Les objets correspondants sont alors ignorés lors de la recherche en temps réel. La protection temps réel peut ignorer via la liste des processus à exclure leurs accès aux fichiers lors de la recherche en temps réel. Ceci est utile notamment pour les bases de données ou solutions de sauvegarde. (Options disponibles uniquement si le mode expert est activé.)

Tenez compte de ce qui suit lors de l'indication des processus et objets de fichiers à exclure : la liste est traitée de haut en bas. Plus la liste est longue, plus le temps processeur nécessaire au traitement de la liste pour chaque accès augmente. Gardez la liste aussi courte que possible.

Processus à exclure par la protection temps réel

Tous les accès aux fichiers par les processus de cette liste sont exclus de la surveillance par la protection temps réel.

Champ de saisie

Dans ce champ, saisissez le nom du processus qui doit être ignoré lors de la recherche en temps réel. Aucun processus n'est indiqué par défaut.

Le chemin indiqué et le nom de fichier du processus peuvent contenir 255 signes au maximum. Vous pouvez saisir jusqu'à 128 processus. Les entrées de la liste ne doivent pas dépasser 6 000 caractères au total.

Les caractères Unicode sont acceptés pour indiquer le processus. Vous pouvez par conséquent saisir des noms de processus ou de répertoires contenant des caractères spéciaux.

Les lecteurs doivent être indiqués comme suit : `[lettre du lecteur]:\`

Le caractère deux-points (:) ne peut être utilisé que pour indiquer des lecteurs.

Pour indiquer le processus, vous pouvez utiliser les caractères de remplacement * (un nombre illimité de caractères) et ? (un seul caractère) :




```
C:\Programmes\Application\application.exe
C:\Programmes\Application\applicatio?.exe
C:\Programmes\Application\applica*.exe
C:\Programmes\Application\*.exe
```

Pour éviter d'exclure des processus globalement de la surveillance de la protection temps réel, les indications comprenant exclusivement les caractères suivants ne sont pas valables : * (étoile), ? (point d'interrogation), / (barre oblique), \ (barre oblique inversée), . (point), : (deux-points).

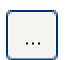
Vous avez la possibilité d'exclure des processus de la surveillance de la protection temps réel sans en indiquer complètement le chemin : `application.exe`

Cela s'applique toutefois exclusivement aux processus dont les fichiers exécutables se trouvent sur les lecteurs du disque dur.

Il est nécessaire d'indiquer complètement le chemin des processus dont les fichiers exécutables se trouvent sur des lecteurs connectés, par ex. des lecteurs réseau. Tenez compte à ce sujet des remarques générales sur l'indication des exceptions sur des lecteurs réseau connectés.

N'indiquez aucune exception pour les processus dont les fichiers exécutables se trouvent sur des lecteurs dynamiques. Les lecteurs dynamiques sont utilisés pour des supports de données tels que des CD, DVD ou clé USB.

Avertissement
Notez que tous les accès aux fichiers initiés par les processus inclus dans la liste sont exclus de la recherche de virus et de programmes indésirables.



Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner un fichier exécutable.

Processus

Le bouton « **Processus** » ouvre la fenêtre « *Sélection de processus* », dans laquelle les processus en cours sont affichés.

Ajouter

Ce bouton vous permet de valider dans la fenêtre d'affichage le processus entré dans le champ de saisie.

Supprimer

Ce bouton vous permet de supprimer un processus sélectionné de la fenêtre d'affichage.

Objets de fichiers à exclure par la protection temps réel



Tous les accès fichiers aux objets de cette liste sont exclus de la surveillance par la protection temps réel.

Champ de saisie

Entrez dans ce champ le nom de l'objet de fichier qui doit être ignoré par la recherche en temps réel. Aucun objet de fichier n'est indiqué par défaut.

Les entrées de la liste ne doivent pas dépasser 6 000 caractères au total.

Pour indiquer les objets de fichiers à exclure, vous pouvez utiliser les caractères de remplacement * (un nombre illimité de caractères) et ? (un seul caractère). Des extensions de fichiers individuelles peuvent aussi être exclues (y compris avec des caractères de remplacement) :

```
C:\Répertoire\*.mdb
*.mdb
*.md?
*.xls*
C:\Répertoire\*.log
```

Les noms de répertoires doivent se terminer par une barre oblique inversée \.

Lorsqu'un répertoire est exclu, tous ses sous-répertoires sont aussi ignorés automatiquement.

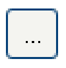
Vous pouvez indiquer 20 exceptions au maximum par lecteur avec le chemin complet (commençant par la lettre du lecteur).

Ex. : `C:\Programmes\Application\Nom.log`

Le nombre maximum d'exceptions sans chemin complet s'élève à 64. Ex. :

```
*.log
\Ordinateur1\C\Répertoire1
```

Pour les lecteurs dynamiques qui sont connectés (mounted) en tant que répertoire d'un autre lecteur, vous devez utiliser, dans la liste des exceptions, l'alias du système d'exploitation pour le lecteur relié :
ex. `\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1`
Si vous utilisez le point de montage (mount point) lui-même, par ex. `C:\DynDrive`, le lecteur dynamique est malgré tout contrôlé. Vous pouvez déterminer l'alias du système d'exploitation à utiliser, à partir du fichier rapport de la protection temps réel.



Ce bouton ouvre une fenêtre dans laquelle vous pouvez sélectionner l'objet de fichier à exclure.

Ajouter

Ce bouton vous permet de reprendre dans la fenêtre d'affichage l'objet de fichier entré dans le champ de saisie.



Supprimer

Le bouton Supprimer vous permet de supprimer un objet de fichier sélectionné de la fenêtre d'affichage.

Tenez compte des autres remarques pour indiquer les exceptions

Pour exclure des objets également lors d'un accès avec un nom de fichier DOS court (convention de noms DOS 8.3), le nom de fichier court correspondant doit aussi être saisi dans la liste.

Un nom de fichier contenant des caractères de remplacement ne doit pas se terminer par une barre oblique inversée.
Par exemple :
`C:\Programmes\Application\applic*.exe\`
Cette entrée n'est pas valable et n'est pas considérée comme une exception.

Tenez compte de ce qui suit pour les **exceptions sur des lecteurs réseau connectés** : si vous utilisez la lettre du lecteur connecté, les fichiers et répertoires indiqués ne sont PAS exclus de la recherche effectuée par la protection temps réel. Si le chemin UNC figurant dans la liste des exceptions est différent de celui utilisé pour connecter le lecteur réseau (indication de l'adresse IP dans la liste des exceptions – indication du nom de l'ordinateur pour la connexion avec le lecteur réseau), les fichiers et répertoires indiqués ne sont PAS exclus de la recherche effectuée par la protection temps réel. Déterminez le chemin UNC à utiliser à l'aide du fichier rapport de la protection temps réel :
`\\<Nom_ordinateur>\<Partage>\` -OU- `\\<Adresse IP>\<Partage>\`

Vous pouvez déterminer les chemins utilisés par la protection temps réel lors de la recherche de fichiers contaminés, à partir du fichier rapport de la protection temps réel. Utilisez systématiquement les mêmes chemins dans la liste des exceptions. Réglez la fonction de consignation de la protection temps réel sur **Intégrale** dans la configuration sous Rapport. La protection temps réel étant activée, accédez maintenant aux fichiers, répertoires, lecteurs intégrés ou lecteurs réseau connectés. Vous pouvez maintenant lire le chemin à utiliser à partir du fichier rapport de la protection temps réel. Vous consultez le fichier rapport dans le Control Center sous Protection temps réel.

Heuristique

Cette rubrique de configuration contient les paramètres pour l'heuristique du moteur de recherche. (Option disponible uniquement si le mode expert est activé.)

Les produits Avira contiennent des heuristiques très performantes qui permettent de détecter dynamiquement des logiciels malveillants inconnus, c'est-à-dire avant même qu'une signature de virus spéciale n'ait été créée contre le parasite et qu'une mise à jour de protection antivirus correspondante n'ait été envoyée. La détection des virus s'effectue par une analyse complexe et un examen du code en cause, à la recherche de fonctions typiques des logiciels malveillants. Si le code examiné présente ces caractéristiques, il est signalé comme suspect. Cela ne signifie pas obligatoirement que le code est un logiciel



malveillant ; des messages erronés peuvent aussi survenir. C'est l'utilisateur qui doit décider comment traiter le code, par ex. sur la base de ses connaissances pour savoir si la source contenant le code signalé est digne de confiance.

Heuristique de macrovirus

Heuristique de macrovirus

Votre produit Avira contient une heuristique de macrovirus très performante. Si l'option est activée, toutes les macros du document contaminé sont supprimées si une réparation est possible ; les documents suspects peuvent aussi être seulement signalés, c'est-à-dire que vous recevez un avertissement. Ce paramètre est activé par défaut et recommandé.

Advanced Heuristic Analysis and Detection (AHeAD)

Activer AHeAD

Votre programme Avira contient une heuristique très performante grâce à la technologie Avira AHeAD, lui permettant de détecter aussi les (nouveaux) logiciels malveillants inconnus. Si l'option est activée, vous pouvez régler ici la sensibilité de cette heuristique. Ce paramètre est activé par défaut.

Niveau de détection bas

Si l'option est activée, moins de logiciels malveillants inconnus sont détectés, le risque de détections erronées est faible dans ce cas.

Niveau de détection moyen

Si l'option est activée, une protection équilibrée est assurée avec peu de messages d'erreurs. Ce paramètre est activé par défaut si vous avez choisi l'utilisation de cette heuristique.

Niveau de détection élevé

Si l'option est activée, nettement plus de logiciels malveillants inconnus sont détectés, sachant qu'il faut toutefois s'attendre à des messages erronés.

12.2.2 Rapport

La protection temps réel dispose d'une fonction étendue de consignation qui peut donner à l'utilisateur et à l'administrateur des indications exactes sur un résultat positif. (Option disponible uniquement si le mode expert est activé.)

Consignation

Ce groupe permet de définir le contenu du fichier rapport.



Désactivée

Si l'option est activée, la protection temps réel ne génère pas de rapport.
Ne renoncez à la consignation que dans des cas exceptionnels, par ex. uniquement lorsque vous effectuez des tests avec de nombreux virus ou programmes indésirables.

Par défaut

Si l'option est activée, la protection temps réel consigne les informations importantes (sur les résultats positifs, les avertissements et les erreurs) dans le fichier rapport, les informations secondaires sont ignorées pour une meilleure lisibilité. Ce paramètre est activé par défaut.

Étendue

Si l'option est activée, la protection temps réel consigne également les informations secondaires dans le fichier rapport.

Intégrale

Si l'option est activée, la protection temps réel consigne toutes les informations dans le fichier rapport, même celles sur la taille et le type des fichiers, la date, etc.

Limiter le fichier rapport

Limiter la taille à n Mo

Si l'option est activée, il est possible de limiter la taille du fichier rapport ; valeurs possibles : 1 à 100 Mo. En cas de limitation du fichier rapport, une marge d'environ 50 kilo-octets est laissée pour ne pas trop solliciter l'ordinateur. Si la taille du fichier rapport dépasse la taille indiquée de 50 kilo-octets, les anciennes entrées sont supprimées automatiquement jusqu'à ce que la taille indiquée moins 50 kilo-octets soit atteinte.

Sauvegarder le fichier rapport avant de le raccourcir

Si l'option est activée, le fichier rapport est sauvegardé avant d'être raccourci.

Écrire la configuration dans le fichier rapport

Si l'option est activée, la configuration de la recherche en temps réel utilisée est écrite dans le fichier rapport.

Remarque
Si vous n'avez indiqué aucune limitation du fichier rapport, un nouveau fichier est automatiquement créé lorsque le fichier rapport a atteint une taille de 100 Mo. Une sauvegarde de l'ancien fichier rapport est créée. Jusqu'à trois sauvegardes des anciens fichiers rapport sont conservées. Les sauvegardes les plus anciennes sont supprimées.



12.3 Mise à jour

La rubrique **Mise à jour** vous permet de configurer l'exécution automatique de mises à jour. Vous avez la possibilité de régler différents intervalles de mise à jour.

Mise à jour automatique

tous les n jours / heures / minutes

Dans ce champ, vous pouvez indiquer l'intervalle auquel les mises à jour automatiques doivent être exécutées. Pour modifier l'intervalle de mise à jour, sélectionnez l'une des indications de temps dans le champ et modifiez-la via les touches fléchées à droite du champ de saisie.

Démarrer également la tâche quand une connexion Internet est établie

Si l'option est activée, en plus de l'intervalle de mise à jour défini, la tâche de mise à jour est exécutée à chaque démarrage d'une connexion Internet. (Option disponible uniquement si le mode expert est activé.)

Rattraper la tâche quand la date est déjà passée

Si l'option est activée, le programme effectue les tâches de mise à jour situées dans le passé qui n'ont pas pu être exécutées au moment voulu, par ex. parce que l'ordinateur était éteint. (Option disponible uniquement si le mode expert est activé.)

12.3.1 Serveur Web

Serveur Web

La mise à jour peut être effectuée directement via un serveur Web sur Internet . (Options disponibles uniquement si le mode expert est activé.)

Connexion au serveur Web

Utiliser la connexion existante (réseau)

Ce paramètre s'affiche lorsque votre connexion est utilisée via un réseau.

Utiliser la connexion suivante

Ce paramètre s'affiche lorsque vous définissez votre connexion individuellement.

L'Updater détecte automatiquement quelles options de connexion sont disponibles. Les options de connexion indisponibles sont grisées et ne peuvent pas être activées. Vous pouvez établir une connexion de télétransmission p. ex. manuellement sous Windows par une entrée de répertoire téléphonique.

Utilisateur

Saisissez l'identifiant du compte sélectionné.

Mot de passe

Saisissez le mot de passe pour ce compte. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*).

> **Remarque**
> Adressez-vous au fournisseur d'accès Internet si vous avez oublié l'identifiant ou le mot de passe d'un compte Internet existant.

> **Remarque**
> La composition automatique de l'Updater via des outils de numérotation (par ex. SmartSurfer, Oleco,...) n'est pas encore disponible.

Arrêter une connexion de télétransmission ouverte pour la mise à jour

Si cette option est activée, la connexion de télétransmission ouverte pour la mise à jour est interrompue automatiquement dès que le téléchargement est terminé.

> **Remarque**
> Cette option n'est disponible que sous Windows XP. À partir de Windows Vista, la connexion de télétransmission ouverte pour la mise à jour est systématiquement interrompue, dès que le téléchargement est terminé.

Paramètres proxy

Serveur proxy

Ne pas utiliser de serveur proxy

Si cette option est activée, votre connexion au serveur Web n'a pas lieu via un serveur proxy.

Utiliser les paramètres système de Windows

Si cette option est activée, les paramètres système actuels de Windows pour la connexion au serveur Web via un serveur proxy sont utilisés. Vous configurez les paramètres système de Windows pour l'utilisation d'un serveur proxy sous **Panneau de configuration > Options Internet > Connexions > Paramètres LAN**. Vous pouvez également accéder aux options Internet dans le menu **Extras** d'Internet Explorer.

> **Avertissement**
> Si vous utilisez un serveur proxy qui exige une authentification, indiquez les données complètes sous l'option **Connexion via ce proxy**. L'option **Utiliser les**



paramètres système de Windows ne peut être utilisée que pour les serveurs proxy sans authentification.

Connexion via ce serveur proxy

Si l'option est activée, votre connexion au serveur Web a lieu via un serveur proxy, selon les paramètres que vous avez indiqués.

Adresse

Saisissez le nom de l'ordinateur ou l'adresse IP du serveur proxy que vous souhaitez utiliser pour la connexion au serveur Web.

Port

Saisissez le numéro de port du serveur proxy que vous souhaitez utiliser pour la connexion au serveur Web.

Identifiant de connexion

Saisissez un identifiant pour la connexion au serveur proxy.

Mot de passe de connexion

Saisissez le mot de passe correspondant pour la connexion au serveur proxy. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*).

Exemples :

Adresse : `proxy.domaine.fr` Port : `8080`

Adresse : `192.168.1.100` Port : `3128`

12.4 Sauvegarde

Vous pouvez configurer le composant de sauvegarde sous **Configuration > Sécurité Internet > Sauvegarde**. (Options disponibles uniquement si le mode expert est activé.)

12.4.1 Paramètres

Vous pouvez configurer le comportement du composant de sauvegarde sous la rubrique **Paramètres**.

Sauvegarder uniquement les fichiers modifiés

Si l'option est activée, une sauvegarde incrémentielle est créée : sont sauvegardés uniquement les fichiers du profil de sauvegarde qui ont été modifiés depuis la dernière sauvegarde de données. Si l'option est désactivée, une sauvegarde complète est effectuée à chaque sauvegarde d'un profil de sauvegarde : tous les fichiers correspondant au profil de sauvegarde sont sauvegardés. Cette option, activée par défaut, est recommandée, car les sauvegardes incrémentielles sont créées plus

rapidement et en utilisant moins de ressources que les sauvegardes complètes de données.

Contrôler l'absence de logiciels malveillants avant la sauvegarde

Si l'option est activée, l'absence de virus et de logiciels malveillants est contrôlée dans les fichiers à sauvegarder. Les fichiers contaminés ne sont pas sauvegardés. Cette option, activée par défaut, est recommandée.

12.4.2 Exceptions

Sous **Exceptions**, vous pouvez déterminer quels objets et types de fichiers doivent être sauvegardés ou non lors d'une sauvegarde.

Objets de fichiers à exclure par la sauvegarde

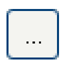
La liste affichée dans cette fenêtre contient des fichiers et chemins qui ne doivent pas être sauvegardés lors d'une sauvegarde.

Remarque
Les entrées de la liste ne doivent pas dépasser 6 000 caractères au total.

Remarque
Les fichiers inscrits dans cette liste sont mentionnés dans le fichier rapport.

Champ de saisie

Saisissez dans ce champ le nom de l'objet de fichier qui ne doit pas être sauvegardé. Le chemin du répertoire temporaire correspondant aux paramètres locaux de l'utilisateur connecté est indiqué par défaut.



Ce bouton ouvre une fenêtre dans laquelle vous pouvez sélectionner le fichier ou le chemin souhaité.
Si vous saisissez un nom de fichier avec son chemin complet, c'est exactement ce fichier qui n'est pas sauvegardé. Si vous avez inscrit le nom d'un fichier sans son chemin, chaque fichier de ce nom (quel que soit son chemin ou le lecteur sur lequel il se situe) n'est pas sauvegardé.

Ajouter

Ce bouton vous permet de reprendre dans la fenêtre d'affichage l'objet de fichier entré dans le champ de saisie.

Supprimer

Le bouton supprime une entrée sélectionnée de la liste. Ce bouton n'est pas actif si aucune entrée n'est sélectionnée.

Réinitialiser la liste

Ce bouton restaure les valeurs définies par défaut.

Tenez compte des points suivants

- Les caractères de remplacement * (un nombre illimité de caractères) et ? (un seul caractère) sont autorisés uniquement dans les noms de fichiers.
- La liste est traitée de haut en bas.
- Lorsqu'un répertoire est exclu, tous ses sous-répertoires sont aussi ignorés automatiquement.
- Des extensions de fichiers individuelles peuvent aussi être exclues (y compris avec des caractères de remplacement).
- Pour exclure des objets également lors d'un accès avec un nom de fichier DOS court (convention de noms DOS 8.3), le nom de fichier court correspondant doit aussi être saisi dans la liste.

Remarque
Un nom de fichier contenant des caractères de remplacement ne doit pas se terminer par une barre oblique inversée. Par exemple :
`C:\Programmes\Application\applic*.exe\`
Cette entrée n'est pas valable et n'est pas considérée comme une exception !

Exemples

- `application.exe`
- `\Programmes\`
- `C:\*.*`
- `C:\*`
- `*.exe`
- `*.xl?`
- `*.*`
- `C:\Programmes\Application\application.exe`
- `C:\Programmes\Application\applic*.exe`
- `C:\Programmes\Application\applic*`
- `C:\Programmes\Application\applic?????.e*`
- `C:\Programmes\`
- `C:\Programmes`
- `C:\Programmes\Application\*.mdb`

Liste des extensions de fichiers

Prendre en compte toutes les extensions de fichiers

Si l'option est activée, tous les fichiers du profil de sauvegarde sont sauvegardés.

Activer la liste des extensions de fichiers à exclure

Si l'option est activée, tous les fichiers du profil de sauvegarde sont sauvegardés, à l'exception des fichiers dont les extensions figurent dans la liste des extensions de fichiers à exclure.

Extensions de fichiers

Ce bouton permet de faire apparaître une fenêtre de dialogue dans laquelle s'affichent toutes les extensions de fichiers qui sont ignorées lors d'une sauvegarde si l'option « **Activer la liste des extensions de fichiers à exclure** » est activée. Pour les extensions, des entrées sont indiquées par défaut, mais il est possible d'ajouter et de supprimer des entrées.

Activer la liste des extensions de fichiers à inclure

Si l'option est activée, seuls les fichiers dont les extensions figurent dans la liste des extensions de fichiers à inclure sont sauvegardés.

Extensions de fichiers

Ce bouton permet de faire apparaître une boîte de dialogue dans laquelle s'affichent toutes les extensions de fichiers qui sont sauvegardées lors d'une sauvegarde si l'option « **Activer la liste des extensions de fichiers à inclure** » est activée. Pour les extensions, des entrées sont indiquées par défaut, mais il est possible d'ajouter et de supprimer des entrées.

12.4.3 Rapport

Le composant de sauvegarde dispose d'une fonction étendue de consignation.

Consignation

Ce groupe permet de définir le contenu du fichier rapport.

Désactivée

Si l'option est activée, le composant de sauvegarde ne génère pas de rapport. Ne renoncez à la consignation que dans des cas exceptionnels.

Par défaut

Si l'option est activée, le composant de sauvegarde consigne les informations importantes (sur la sauvegarde, sur les virus détectés, les avertissements et les erreurs) dans le fichier rapport, les informations secondaires sont ignorées pour une meilleure lisibilité. Ce paramètre est activé par défaut.

Étendue

Si l'option est activée, le composant de sauvegarde consigne également les informations secondaires dans le fichier rapport.

Intégrale

Si l'option est activée, le composant de sauvegarde consigne toutes les informations concernant l'historique de la sauvegarde et la recherche de virus dans le fichier rapport.

12.5 FireWall

12.5.1 Configuration de l'Avira FireWall

Avira Internet Security vous permet de configurer l'Avira FireWall :

- Avira FireWall

12.5.2 Avira FireWall

La rubrique **FireWall** sous **Configuration > Sécurité Internet** permet de configurer l'Avira FireWall dans les systèmes d'exploitation jusqu'à Windows 7.

Règles d'adaptation

On appelle adaptateur dans l'Avira FireWall chacune des unités matérielles simulées par un logiciel (par ex. miniport, montage en pont, etc.) ou chaque unité matérielle (par ex. une carte réseau).

L'Avira FireWall indique les règles d'adaptation pour tous les adaptateurs existants sur votre ordinateur et pour lesquels un pilote est installé. (Options disponibles uniquement si le mode expert est activé.)

- Protocole ICMP
- Scannage de ports TCP
- Scannage de ports UDP
- Règles entrantes
- Règles sortantes
- Boutons

Une règle d'adaptation prédéfinie dépend du niveau de sécurité. Vous pouvez modifier le *niveau de sécurité* via la rubrique **Sécurité Internet > FireWall** du Control Center ou adapter les règles d'adaptation à vos besoins. Si vous avez adapté les règles d'adaptation à vos besoins, sous la rubrique FireWall du Control Center, le régulateur est placé sur *Utilisateurs* dans la zone **Niveau de sécurité**.

> **Remarque**
> Le paramètre par défaut du niveau de sécurité pour toutes les règles prédéfinies de l'Avira FireWall est **Moyen**.

Protocole ICMP

L'Internet Control Message Protocol (ICMP) sert à l'échange de messages d'erreur et d'information dans les réseaux. Le protocole est aussi utilisé pour les messages d'état par ping ou tracert.
Cette règle vous permet de définir les types d'ICMP entrants et sortants qui doivent être bloqués, de fixer les paramètres de flooding et de définir le comportement en présence de paquets ICMP fragmentés. Cette règle sert à empêcher les attaques par inondation ICMP qui peuvent conduire à la surcharge du processeur de l'ordinateur attaqué car une réponse est donnée à chaque paquet.

Règles prédéfinies pour le protocole ICMP

Paramètre	Règles
Bas	Bloque les types entrants : **aucun type**. Bloque les types sortants : **aucun type.** Suspecter un flooding si le délai entre les paquets est inférieur à **50** millisecondes. **Refuser** les paquets ICMP fragmentés.
Moyen	Mêmes règles que pour le paramètre *Bas*.
Élevé	Bloque les types entrants : **différents types**. Bloque les types sortants : **différents types**. Suspecter un flooding si le délai entre les paquets est inférieur à **50** millisecondes. **Refuser** les paquets ICMP fragmentés.

Types entrants bloqués : aucun type / différents types

Cliquez sur le lien pour ouvrir une liste avec les types de paquets ICMP. Dans cette liste, vous pouvez sélectionner les types de messages ICMP entrants que vous souhaitez bloquer.



Types sortants bloqués : aucun type / différents types

Cliquez sur le lien pour ouvrir une liste avec les types de paquets ICMP. Dans cette liste, vous pouvez sélectionner les types de messages ICMP sortants que vous souhaitez bloquer.

Suspecter un flooding

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir la valeur maximale autorisée pour le délai ICMP.

Paquets ICMP fragmentés

En cliquant sur le lien, vous avez la possibilité de choisir entre « **refuser** » et « **ne pas refuser** » des paquets ICMP fragmentés.

Scannage de ports TCP

Cette règle vous permet de définir quand le FireWall doit suspecter un scannage de ports TCP et comment il doit se comporter dans ce cas. Cette règle sert à empêcher les attaques par scannage de ports TCP qui peuvent être constatées via les ports ouverts sur votre ordinateur. Les attaques de ce type sont surtout utilisées pour exploiter les faiblesses de votre ordinateur afin de pouvoir opérer des attaques beaucoup plus dangereuses.

Règles prédéfinies pour le scannage de ports TCP

Paramètre	Règles
Bas	Suspecter un scannage de ports TCP si **50** ports au moins ont été scannés en **5000** millisecondes. Lors de la détection d'un scannage de ports TCP, écrire l'adresse IP de l'agresseur **dans la base de données d'événements** et **ne pas l'ajouter** aux règles pour bloquer l'attaque.
Moyen	Suspecter un scannage de ports TCP si **50** ports au moins ont été scannés en **5000** millisecondes. Lors de la détection d'un scannage de ports TCP, écrire l'adresse IP de l'agresseur **dans la base de données d'événements** et l'**ajouter** aux règles pour bloquer l'attaque.
Élevé	Mêmes règles que pour le paramètre *Moyen*.

Ports

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir le nombre de ports qui doivent avoir été scannés pour qu'un scannage de ports TCP soit suspecté.

Intervalle de scannage de ports

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir l'intervalle pendant lequel un nombre défini de ports doit avoir été scanné pour qu'un scannage de ports TCP soit suspecté.

Base de données d'événements

Cliquez sur ce lien pour avoir la possibilité de choisir si l'adresse IP de l'agresseur doit être inscrite ou non dans la base de données d'événements.

Règle

Cliquez sur ce lien pour avoir la possibilité de choisir si la règle de blocage de l'attaque par scannage de ports TCP doit être ajoutée ou non.

Scannage de ports UDP

Cette règle vous permet de définir quand le FireWall doit suspecter un scannage des ports UDP et quel doit être son comportement dans ce cas. Cette règle sert à empêcher les attaques par scannage de ports UDP qui peuvent être constatées via les ports ouverts sur votre ordinateur. Les attaques de ce type sont surtout utilisées pour exploiter les faiblesses de votre ordinateur afin de pouvoir opérer des attaques beaucoup plus dangereuses.

Règles prédéfinies pour le scannage de ports UDP

Paramètre	Règles
Bas	Suspecter un scannage de ports UDP si **50** ports au moins ont été scannés en **5000** millisecondes. Lors de la détection d'un scannage de ports UDP, écrire l'adresse IP de l'agresseur **dans la base de données d'événements** et **ne pas l'ajouter** aux règles pour bloquer l'attaque.
Moyen	Suspecter un scannage de ports UDP si **50** ports au moins ont été scannés en **5000** millisecondes. Lors de la détection d'un scannage de ports TCP, écrire l'adresse IP de l'agresseur **dans la base de données d'événements** et l'**ajouter** aux règles pour bloquer l'attaque.
Élevé	Même règle que pour le paramètre *Moyen*.

Ports

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir le nombre de ports qui doivent avoir été scannés pour qu'un scannage de ports UDP soit suspecté.



Intervalle de scannage de ports

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir l'intervalle pendant lequel un nombre défini de ports doit avoir été scanné pour qu'un scannage de ports UDP soit suspecté.

Base de données d'événements

Cliquez sur ce lien pour avoir la possibilité de choisir si l'adresse IP de l'agresseur doit être inscrite ou non dans la base de données d'événements.

Règle

Cliquez sur ce lien pour avoir la possibilité de choisir si la règle de blocage de l'attaque par scannage de ports UDP doit être ajoutée ou non.

Règles entrantes

Les règles entrantes servent au contrôle du trafic de données entrant par l'Avira FireWall.

> **Avertissement**
> Étant donné que, lors du filtrage d'un paquet, les règles correspondantes sont appliquées les unes après les autres, leur ordre est important. Ne modifiez l'ordre des règles que si vous êtes certain du résultat que vous souhaitez obtenir.

Règles prédéfinies pour la surveillance du trafic de données TCP



Paramètre	Règles
Bas	Le trafic de données entrant n'est pas bloqué par l'Avira FireWall.
Moyen	• **Autoriser la connexion TCP existante sur le port 135** **Autoriser** les paquets TCP, de l'adresse **0.0.0.0** avec le masque **0.0.0.0** lorsque le port local se trouve sur **{135}** et le port distant sur **{0-65535}**. Appliquer aux **paquets de connexions existantes**. **Ne pas écrire dans la base de données d'événements** si le paquet correspond à la règle. Étendu : sélectionner les paquets contenant les octets suivants **<vide>** avec le masque **<vide>** sur le décalage **0**. • **Rejeter les paquets TCP sur le port 135** **Refuser** les paquets TCP, de l'adresse **0.0.0.0** avec le masque **0.0.0.0** quand le port local est sur **{135}** et le port distant sur **{0-65535}**. Appliquer à **tous les paquets**. **Ne pas écrire dans la base de données d'événements** si le paquet correspond à la règle. Étendu : sélectionner les paquets contenant les octets suivants **<vide>** avec le masque **<vide>** sur le décalage **0**. • **Surveiller le trafic de données TCP conforme** **Autoriser** les paquets TCP, de l'adresse **0.0.0.0** avec le masque **0.0.0.0** lorsque le port local se trouve sur **{0-65535}** et le port distant sur **{0-65535}**. Appliquer au **début de l'établissement de la connexion et aux paquets des connexions existantes**. **Ne pas écrire dans la base de données d'événements** si le paquet correspond à la règle. Étendu : sélectionner les paquets contenant les octets suivants **<vide>** avec le masque **<vide>** sur le décalage **0**. • **Rejeter tous les paquets TCP** **Refuser** les paquets TCP, de l'adresse **0.0.0.0** avec le masque **0.0.0.0** quand le port local est sur **{0-65535}** et le port distant sur **{0-65535}**. Appliquer à **tous les paquets**. **Ne pas écrire dans la base de données d'événements** si le paquet correspond à la règle. Étendu : sélectionner les paquets contenant les octets suivants **<vide>** avec le masque **<vide>** sur le décalage **0**.

Élevé	**Surveiller le trafic de données TCP autorisé** **Autoriser** les paquets TCP, de l'adresse **0.0.0.0** avec le masque **0.0.0.0** lorsque le port local se trouve sur **{0-65535}** et le port distant sur **{0-65535}**. Appliquer aux **paquets de connexions existantes**. **Ne pas écrire dans la base de données d'événements** si le paquet correspond à la règle. Étendu : sélectionner les paquets contenant les octets suivants **<vide>** avec le masque **<vide>** sur le décalage **0**.

Autoriser / refuser les paquets TCP

En cliquant sur le lien, vous avez la possibilité de décider si vous souhaitez autoriser ou rejeter les paquets TCP spécialement définis.

Adresse IP

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir l'adresse IPv4 ou IPv6 souhaitée.

Masque IP

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir le masque IPv4 ou IPv6 souhaité.

Ports locaux

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir un ou plusieurs ports locaux souhaités ainsi que des plages entières de ports.

Ports distants

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir un ou plusieurs ports distants souhaités ainsi que des plages entières de ports.

Méthode d'application

En cliquant sur le lien, vous avez la possibilité de choisir si la règle doit être appliquée aux paquets de connexions existantes, au début de l'établissement de la connexion, et aux paquets de connexions existantes ou à toutes les connexions.

Base de données d'événements

En cliquant sur le lien, vous avez la possibilité de choisir d'écrire ou non dans la base de données d'événements si le paquet correspond à la règle.

Étendue

L'option **Étendu** permet un filtrage sur la base du contenu. Ainsi, vous pouvez par exemple refuser des paquets qui contiennent des données spécifiques avec un

décalage défini. Si vous ne souhaitez pas utiliser cette option, ne sélectionnez aucun fichier ou sélectionnez un fichier vide.

Filtrage en fonction du contenu : octets

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez sélectionner le fichier contenant la mémoire tampon spéciale.

Filtrage en fonction du contenu : masque

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez sélectionner le masque spécial.

Filtrage en fonction du contenu : décalage

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez indiquer le décalage pour le filtrage du contenu. Le décalage est calculé à partir de la fin de l'en-tête TCP.

Règles prédéfinies pour la surveillance du trafic de données UDP

Paramètre	Règles
Bas	-
Moyen	• **Surveiller le trafic de données UDP conforme** **Autoriser** les paquets UDP de l'adresse **0.0.0.0** avec le masque **0.0.0.0**, lorsque le port local se trouve sur **{0-65535}** et le port distant sur **{0-65535}**. Appliquer la règle aux **ports ouverts** pour **tous les flux de données**. **Ne pas écrire dans la base de données d'événements** si le paquet correspond à la règle. Étendu : sélectionner les paquets contenant les octets suivants **<vide>** avec le masque **<vide>** sur le décalage **0**. • **Rejeter tous les paquets UDP** **Refuser** les paquets TCP, de l'adresse **0.0.0.0** avec le masque **0.0.0.0** quand le port local est sur **{0-65535}** et le port distant sur **{0-65535}**. Appliquer la règle à **tous les ports** pour **tous les flux de données**. **Ne pas écrire dans la base de données d'événements** si le paquet correspond à la règle. Étendu : sélectionner les paquets contenant les octets suivants **<vide>** avec le masque **<vide>** sur le décalage **0**.

Élevé	**Surveiller le trafic de données UDP autorisé** **Autoriser** les paquets UDP de l'adresse **0.0.0.0** avec le masque **0.0.0.0**, lorsque le port local se trouve sur **{0-65535}** et le port distant sur **{53, 67, 68, 88,...}**. Appliquer la règle aux **ports ouverts** pour **tous les flux de données**. **Ne pas écrire dans la base de données d'événements** si le paquet correspond à la règle. Étendu : sélectionner les paquets contenant les octets suivants **<vide>** avec le masque **<vide>** sur le décalage **0**.

Autoriser / refuser les paquets UDP

En cliquant sur le lien, vous avez la possibilité d'autoriser ou de rejeter les paquets UDP spécialement définis.

Adresse IP

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir l'adresse IPv4 ou IPv6 souhaitée.

Masque IP

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir le masque IPv4 ou IPv6 souhaité.

Ports locaux

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir un ou plusieurs ports locaux souhaités ainsi que des plages entières de ports.

Ports distants

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir un ou plusieurs ports distants souhaités ainsi que des plages entières de ports.

Méthode d'application

Ports

En cliquant sur ce lien, vous pouvez choisir si la règle doit s'appliquer à tous les ports ou uniquement à tous les ports ouverts.

Flux de données

En cliquant sur ce lien, vous pouvez choisir si la règle doit s'appliquer à tous les flux de données ou uniquement aux flux de données sortants.

Base de données d'événements

En cliquant sur le lien, vous avez la possibilité de choisir d'écrire ou non dans la base de données d'événements si le paquet correspond à la règle.



Étendue

L'option **Étendu** permet un filtrage sur la base du contenu. Ainsi, vous pouvez par exemple refuser des paquets qui contiennent des données spécifiques avec un décalage défini. Si vous ne souhaitez pas utiliser cette option, ne sélectionnez aucun fichier ou sélectionnez un fichier vide.

Filtrage en fonction du contenu : octets

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez sélectionner le fichier contenant la mémoire tampon spéciale.

Filtrage en fonction du contenu : masque

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez sélectionner le masque spécial.

Filtrage en fonction du contenu : décalage

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez indiquer le décalage pour le filtrage du contenu. Le décalage est calculé à partir de la fin de l'en-tête UDP.

Règles prédéfinies pour la surveillance du trafic de données ICMP

Paramètre	Règles
Bas	-
Moyen	**Ne rejeter aucun paquet ICMP sur la base de l'adresse IP** **Autoriser** les paquets ICMP de l'adresse **0.0.0.0** avec le masque **0.0.0.0**. **Ne pas écrire dans la base de données d'événements** si le paquet correspond à la règle. Étendu : sélectionner les paquets contenant les octets suivants **<vide>** avec le masque **<vide>** sur le décalage **0**.
Élevé	Même règle que pour le paramètre *Moyen*.

Autoriser / refuser les paquets ICMP

En cliquant sur le lien, vous avez la possibilité d'autoriser ou de rejeter les paquets ICMP spécialement définis.

Adresse IP

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir l'adresse IPv4 souhaitée.

Masque IP

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir le masque IPv4 souhaité.

Base de données d'événements

En cliquant sur le lien, vous avez la possibilité de choisir d'écrire ou non dans la base de données d'événements si le paquet correspond à la règle.

Étendue

L'option **Étendu** permet un filtrage sur la base du contenu. Ainsi, vous pouvez par exemple refuser des paquets qui contiennent des données spécifiques avec un décalage défini. Si vous ne souhaitez pas utiliser cette option, ne sélectionnez aucun fichier ou sélectionnez un fichier vide.

Filtrage en fonction du contenu : octets

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez sélectionner le fichier contenant la mémoire tampon spéciale.

Filtrage en fonction du contenu : masque

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez sélectionner le masque spécial.

Filtrage en fonction du contenu : décalage

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez indiquer le décalage pour le filtrage du contenu. Le décalage est calculé à partir de la fin de l'en-tête ICMP.

Règle prédéfinie pour les paquets IP

Paramètre	Règles
Bas	-
Moyen	-
Élevé	**Rejeter tous les paquets IP** **Refuser** les paquets **IPv4** de l'adresse **0.0.0.0** avec le masque **0.0.0.0**. **Ne pas écrire dans la base de données d'événements** si le paquet correspond à la règle.

Autoriser / refuser

En cliquant sur le lien, vous avez la possibilité d'autoriser ou de rejeter les paquets IP spécialement définis.



IPv4 / IPv6

Cliquez sur le lien pour choisir entre IPv4 ou IPv6.

Adresse IP

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir l'adresse IPv4 ou IPv6 souhaitée.

Masque IP

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir le masque IPv4 ou IPv6 souhaité.

Base de données d'événements

En cliquant sur le lien, vous avez la possibilité de choisir d'écrire ou non dans la base de données d'événements si le paquet correspond à la règle.

Règles sortantes

Les règles sortantes servent au contrôle du trafic de données sortant par l'Avira FireWall. Vous pouvez définir une règle sortante pour les protocoles suivants : IP, ICMP, UDP et TCP.

> **Avertissement**
> Étant donné que, lors du filtrage d'un paquet, les règles correspondantes sont appliquées les unes après les autres, leur ordre est important. Ne modifiez l'ordre des règles que si vous êtes certain du résultat que vous souhaitez obtenir.

Boutons

Bouton	Description
Ajouter	Permet de créer une nouvelle règle. Quand vous cliquez sur ce bouton, la boîte de dialogue « Ajouter une nouvelle règle » s'affiche. Vous pouvez sélectionner de nouvelles règles dans cette boîte de dialogue.
Supprimer	Supprime une règle sélectionnée.
Vers le haut	Déplacement d'une règle sélectionnée d'une position vers le haut, ce qui accroît la priorité de cette règle.
Vers le bas	Déplacement d'une règle sélectionnée d'une position vers le bas, ce qui réduit la priorité de cette règle.

Renommer	Permet de renommer une règle sélectionnée.

Remarque
Vous pouvez ajouter de nouvelles règles pour divers adaptateurs ou pour tous les adaptateurs présents sur l'ordinateur. Pour ajouter une règle d'adaptation à tous les adaptateurs, sélectionnez **Poste de travail** dans la structure affichée des adaptateurs et cliquez sur le bouton **Ajouter**. Voir Ajouter une nouvelle règle.

Remarque
Pour modifier la position d'une règle, vous pouvez également faire glisser la règle sur la position souhaitée, à l'aide de la souris.

Ajouter une nouvelle règle

Vous pouvez sélectionner de nouvelles règles entrantes et sortantes dans cette fenêtre. La règle sélectionnée est validée dans la fenêtre **Règles d'adaptation** avec les informations standard et peut être définie plus spécifiquement à partir de là. Vous disposez d'autres règles en plus des règles entrantes et sortantes.

Règles possibles

Autoriser le réseau peer-to-peer

Autorise les connexions poste à poste : communication TCP entrante sur le port 4662 et communication UDP entrante sur le port 4672

Port TCP

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir le port TCP autorisé.

Port UDP

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir le port UDP autorisé.

Autoriser les connexions VMWARE

Autorise la communication entre les systèmes VMWare

Bloquer l'adresse IP

Bloque l'ensemble du trafic d'une adresse IP particulière

Version IP

Cliquez sur le lien pour choisir entre IPv4 ou IPv6.

Adresse IP

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir l'adresse IPv4 ou IPv6 souhaitée.

Bloquer le sous-réseau

Bloque l'ensemble du trafic d'une adresse IP particulière et d'un masque de sous-réseau

Version IP

Cliquez sur le lien pour choisir entre IPv4 ou IPv6.

Adresse IP

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir l'adresse IP souhaitée.

Masque de sous-réseau

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir le masque de sous-réseau souhaité.

Autoriser l'adresse IP

Autorise l'ensemble du trafic d'une adresse IP particulière

Version IP

Cliquez sur le lien pour choisir entre IPv4 ou IPv6.

Adresse IP

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir l'adresse IP souhaitée.

Autoriser le sous-réseau

Autorise l'ensemble du trafic d'une adresse IP particulière et d'un masque de sous-réseau

Version IP

Cliquez sur le lien pour choisir entre IPv4 ou IPv6.

Adresse IP

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir l'adresse IP souhaitée.

Masque de sous-réseau

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir le masque de sous-réseau souhaité.



Autoriser le serveur Web

Autorise la communication d'un serveur Web sur le port 80 : communication TCP entrante sur le port 80

Port

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir le port utilisé par le serveur Web.

Autoriser les connexions VPN

Autorise les connexions VPN (Virtual Private Network) avec une adresse IP particulière : trafic de données UDP entrant sur x ports, trafic de données TCP entrant sur x ports, trafic de données IP entrant avec les protocoles ESP(50), GRE (47)

Version IP

Cliquez sur le lien pour choisir entre IPv4 ou IPv6.

Adresse IP

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir l'adresse IP souhaitée.

Autoriser la connexion « Remote Desktop »

Autorise les connexions « Remote Desktop » (Remote Desktop Protocol) sur le port 3389

Port

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir le port utilisé pour la connexion Remote Desktop autorisée.

Autoriser la connexion VNC

Autorise les connexions VNC (Virtual Network Computing) sur le port 5900

Port

Cliquez sur le lien pour ouvrir une fenêtre de dialogue dans laquelle vous pouvez saisir le port utilisé pour la connexion VNC autorisée.

Autoriser les partages de fichier et d'imprimante

Autorise l'accès aux partages de fichier et d'imprimante : trafic de données TCP entrant sur le port 137, 139 et trafic de données UDP entrant sur le port 445 d'une adresse IP au choix.

Règles entrantes possibles

- **Règle IP entrante**
- **Règle ICMP entrante**
- **Règle UDP entrante**
- **Règle TCP entrante**

- **Règle de protocole IP entrante**

Règles sortantes possibles

- **Règle IP sortante**
- **Règle ICMP sortante**
- **Règle UDP sortante**
- **Règle TCP sortante**
- **Règle de protocole IP sortante**

> **Remarque**
> Les options disponibles pour les règles entrantes et sortantes possibles sont identiques à celles des règles prédéfinies pour les protocoles correspondants, comme décrit sous FireWall > Règles d'adaptation.

Boutons

Bouton	Description
OK	La règle sélectionnée est validée comme nouvelle règle d'adaptation.
Annuler	La fenêtre se referme sans ajouter de nouvelle règle.

Règles d'applications

Règles d'applications pour l'utilisateur

Cette liste comprend tous les utilisateurs du système. Si vous êtes connecté en tant qu'administrateur, vous pouvez sélectionner l'utilisateur pour lequel vous souhaitez établir des règles. Si vous ne disposez pas de droits privilégiés, la liste ne vous indique que l'utilisateur actuellement connecté.

Application

Ce tableau vous montre la liste des applications pour lesquelles des règles sont définies. La liste indique les paramètres pour chaque application exécutée depuis l'installation de l'Avira FireWall et pour laquelle une règle a été enregistrée.

Vue par défaut

Colonne	Description
Application	Nom de l'application
Connexions actives	Nombre de connexions actives ouvertes par l'application
Action	Indique l'action que l'Avira FireWall exécute automatiquement si l'application utilise le réseau, quelle que soit cette utilisation. Cliquez sur le lien pour passer à un autre type d'action. Les types d'action **Demander**, **Autoriser** ou **Refuser** sont proposés. Le paramètre par défaut est **Demander.**

Configuration étendue

Si vous souhaitez régler individuellement les accès réseau d'une application, vous pouvez créer des règles d'applications spécifiques basées sur les filtres de paquets, semblables aux règles d'adaptation.

- Pour passer à la configuration étendue des règles d'applications, activez tout d'abord le **mode expert**.
- Sous **Configuration > Sécurité Internet > FireWall > Paramètres**, modifiez maintenant le paramètre des *règles d'applications* : activez l'option **Paramètres avancés** et enregistrez le paramètre avec **Appliquer** ou **OK**.
  - ↳ Une colonne supplémentaire **Filtrage** avec l'entrée **Simple** s'affiche alors sous **Configuration > Sécurité Internet > FireWall > Règles d'applications**.

Colonne	Description
Application	Nom de l'application.
Connexions actives	Nombre de connexions actives ouvertes par l'application

Action	Indique l'action que l'Avira FireWall exécute automatiquement si l'application utilise le réseau, quelle que soit cette utilisation. Le paramètre **Filtrage - simple** vous permet de passer à un autre type d'action en cliquant sur le lien. Les types d'action **Demander**, **Autoriser** et **Refuser** sont proposés. Le type d'action **Règles** s'affiche avec le paramètre **Filtrage - Étendu**. Le lien **Règles** ouvre la fenêtre **Règles d'applications étendues**, dans laquelle il est possible d'enregistrer des règles spécifiques pour l'application.
Filtrage	Affiche le type de filtrage. En cliquant sur le lien, vous pouvez passer à un autre filtrage. **Simple** : en cas de filtrage simple, l'action indiquée est exécutée pour toutes les activités réseau de l'application logicielle. **Étendu** : lors du filtrage, le système exécute les règles enregistrées dans la configuration étendue.

- Si vous souhaitez créer des règles d'applications spécifiques pour une application, sous **Filtrage** passez à l'entrée **Étendu**.
  - ↳ L'entrée **Règles** est maintenant affichée dans la colonne **Action**.
- Cliquez sur **Règles** pour accéder à la fenêtre de création de règles d'applications spécifiques.

Règles d'applications spécifiques de la configuration étendue

Les règles d'applications spécifiques vous permettent d'autoriser ou de rejeter un trafic de données spécifique de l'application, ainsi que d'autoriser ou de refuser l'écoute passive de ports individuels. Vous disposez des options suivantes :

Refuser / autoriser l'injection de code

L'injection de code est une technique par laquelle on fait exécuter un code dans l'espace d'adressage d'un autre processus, en forçant ce processus à charger une Dynamic Link Library (DLL). La technique d'injection de code est utilisée entre autres par les logiciels malveillants pour exécuter un code sous le couvert d'un autre programme. Il se peut ainsi que le FireWall ne détecte pas des accès à Internet, par exemple. L'injection de code est autorisée par défaut pour toutes les applications signées.

Autoriser ou refuser l'écoute passive de l'application par des ports

Autoriser ou refuser le trafic de données :

Autoriser ou rejeter des paquets IP entrants et/ou sortants

Autoriser ou rejeter des paquets TCP entrants et/ou sortants

Autoriser ou rejeter des paquets UDP entrants et/ou sortants

Vous pouvez créer autant de règles d'applications que vous le souhaitez pour chaque application. Les règles d'applications sont exécutées dans l'ordre affiché (vous trouverez de plus amples informations sous Règles d'applications étendues).

> **Remarque**
> Si vous modifiez le filtrage d'**Étendu** à **Simple** pour une règle d'application, les règles déjà créées dans la configuration étendue ne sont pas définitivement supprimées, mais seulement désactivées. Si vous repassez au filtrage **Étendu**, les règles d'applications déjà créées sont réactivées et s'affichent dans la fenêtre de la configuration étendue concernant les **règles d'applications**.

Détails de l'application

Cette rubrique affiche les informations détaillées concernant l'application que vous avez sélectionnée dans la liste des applications.

- *Nom* - Nom de l'application.
- *Chemin* - Chemin du fichier exécutable de l'application.

Boutons

Bouton	Description
Ajouter une application	Permet de créer une nouvelle règle d'application. Si vous cliquez sur ce bouton, une boîte de dialogue s'affiche. Vous pouvez maintenant sélectionner une application pour laquelle vous souhaitez créer une règle.
Supprimer une règle	Suppression de la règle d'application sélectionnée.
Afficher les détails	La fenêtre *Propriétés* affiche les informations détaillées concernant l'application que vous avez sélectionnée dans la liste. (Option disponible uniquement si le mode expert est activé.)
Charger à nouveau	Nouveau chargement de la liste des applications avec rejet simultané de toutes les modifications qui viennent d'être apportées aux règles d'applications.



Règles d'applications étendues

La fenêtre **Règles d'applications étendues** vous permet de créer des règles spécifiques pour le trafic de données d'applications et l'écoute de ports. Vous créez une nouvelle règle avec le bouton **Ajouter**. Vous pouvez définir plus spécifiquement la règle dans la zone inférieure de la fenêtre. Vous pouvez créer autant de règles que vous le souhaitez pour une application. Les règles sont exécutées dans l'ordre indiqué. Vous pouvez modifier l'ordre des règles à l'aide des boutons **Vers le haut** et **Vers le bas**.

> **Remarque**
> Pour modifier la position d'une règle d'application, vous pouvez également faire glisser la règle sur la position souhaitée, à l'aide de la souris.

Détails de l'application

La zone Détails de l'application affiche les informations concernant l'application sélectionnée :

- *Nom* - Nom de l'application.
- *Chemin* - Chemin du fichier exécutable de l'application.

Options de règle

Refuser / autoriser l'injection de code

En cliquant sur le lien, vous pouvez déterminer si vous refusez ou autorisez l'injection de code pour l'application sélectionnée.

Type de règle : trafic / écoute

En cliquant sur le lien, vous pouvez définir si vous créez une règle sur le trafic de données ou sur l'écoute de ports.

Action : autoriser / refuser

En cliquant sur le lien, vous pouvez définir quelle action est exécutée avec la règle.

Port

En cliquant sur le lien, une fenêtre de dialogue s'ouvre dans laquelle vous pouvez saisir le port local visé par la règle d'écoute. Vous pouvez également saisir plusieurs ports ou plages de ports.

Paquets sortants, entrants, tous les paquets

En cliquant sur ce lien, vous pouvez définir si la règle de trafic surveille tous les paquets, uniquement les paquets sortants ou uniquement ceux entrants.

Paquets IP / paquets TCP / paquets UDP

En cliquant sur le lien, vous pouvez définir quel protocole est surveillé par la règle de trafic.

Options pour paquets IP

Adresse IP

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir l'adresse IP souhaitée.

Masque IP

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir le masque IP souhaité.

Options pour paquets TCP / paquets UDP

Adresse IP locale

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir l'adresse IP locale souhaitée.

Masque IP local

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir le masque IP local souhaité.

Adresse IP distante

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir l'adresse IP distante souhaitée.

Masque IP distant

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir le masque IP distant souhaité.

Port local

Cliquez sur le lien pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir un ou plusieurs ports locaux souhaités ou bien encore des plages entières de ports.

Port distant

Cliquez sur le lien pour ouvrir une fenêtre de dialogue dans laquelle vous pouvez saisir un ou plusieurs ports distants souhaités ou bien encore des plages entières de ports.

Ne pas écrire dans le fichier rapport / Écrire dans le fichier rapport

En cliquant sur le lien, vous pouvez définir si une entrée est reprise dans le fichier rapport du programme, en cas d'application de la règle.



Boutons

Bouton	Description
Ajouter	Une nouvelle règle d'application est créée.
Supprimer	La règle d'application sélectionnée est effacée.
Vers le haut	La règle d'application sélectionnée se déplace d'une position vers le haut, ce qui augmente la priorité de la règle.
Vers le bas	La règle d'application sélectionnée se déplace d'une position vers le bas, ce qui réduit la priorité de la règle.
Renommer	Permet de modifier le nom de la règle sélectionnée.
Appliquer	Les modifications effectuées sont validées et appliquées directement par l'Avira FireWall.
OK	Les modifications effectuées sont validées. La fenêtre de configuration des règles d'applications se referme.
Annuler	La fenêtre de configuration des règles d'applications se referme sans que les modifications effectuées soient validées.

Fournisseurs dignes de confiance

Une liste des éditeurs de logiciels dignes de confiance s'affiche sous *Fournisseurs dignes de confiance*. (Options disponibles uniquement si le mode expert est activé.)

Vous pouvez supprimer ou ajouter des éditeurs à la liste en utilisant l'option **Toujours faire confiance à ce fournisseur** dans la fenêtre popup **Événement réseau**. Vous pouvez autoriser par défaut l'accès réseau des applications signées par les fournisseurs figurant dans la liste, en activant l'option **Autoriser automatiquement les applications créées par des fournisseurs dignes de confiance**.



Fournisseurs dignes de confiance pour l'utilisateur

Cette liste comprend tous les utilisateurs du système. Si vous êtes connecté en tant qu'administrateur, vous pouvez sélectionner l'utilisateur dont vous souhaitez visualiser ou mettre à jour la liste de fournisseurs dignes de confiance. Si vous ne disposez pas de droits privilégiés, la liste ne vous indique que l'utilisateur actuellement connecté.

Autoriser automatiquement les applications créées par des fournisseurs dignes de confiance

Si l'option est activée, les applications dont la signature provient de fournisseurs connus et dignes de confiance sont automatiquement autorisées à accéder au réseau. L'option est activée par défaut.

Fournisseurs

La liste indique tous les fournisseurs considérés comme dignes de confiance.

Boutons

Bouton	Description
Supprimer	L'entrée sélectionnée est supprimée de la liste des fournisseurs dignes de confiance. Pour supprimer le fournisseur sélectionné définitivement de la liste, cliquez sur **Appliquer** ou **OK** dans la fenêtre de la configuration.
Charger à nouveau	Les modifications apportées sont annulées : la dernière liste enregistrée est chargée.

Remarque
Si vous supprimez des fournisseurs de la liste, puis cliquez sur le bouton **Appliquer**, les fournisseurs sont définitivement effacés de la liste. La modification ne peut pas être annulée avec l'option **Charger à nouveau**. Vous avez toutefois la possibilité d'ajouter de nouveau un éditeur à la liste des fournisseurs dignes de confiance via l'option **Toujours faire confiance à ce fournisseur** dans la fenêtre popup **Événement réseau**.

Remarque
Le FireWall donne la priorité aux règles d'applications avant les entrées figurant dans la liste des fournisseurs dignes de confiance : si vous avez créé une règle d'application et que le fournisseur de l'application figure dans la liste des fournisseurs dignes de confiance, la règle d'application est exécutée.



Paramètres

Options disponibles uniquement si le mode expert est activé.

Paramètres avancés

Désactiver le pare-feu Windows au démarrage

Si l'option est activée, le pare-feu Windows est désactivé au démarrage de l'ordinateur. Cette option est activée par défaut.

Dépassement de délai de la règle

Toujours bloquer

Si l'option est activée, une règle générée automatiquement par exemple lors d'un scannage des ports, est conservée.

Supprimer la règle après n secondes

Si l'option est activée, une règle générée automatiquement lors du scannage des ports par exemple est supprimée après le délai que vous indiquez. Cette option est activée par défaut. Vous pouvez indiquer dans ce champ le nombre de secondes au bout desquelles la règle doit être supprimée.

Notifications

L'option Notifications vous permet de définir les événements pour lesquels vous souhaitez qu'un message du FireWall s'affiche sur le Bureau.

Scannage de ports

Si l'option est activée, un message s'affiche sur le Bureau lorsque le FireWall détecte un scannage de ports.

Flooding

Si l'option est activée, un message s'affiche sur le Bureau lorsque le FireWall détecte une attaque par flooding.

Applications bloquées

Si l'option est activée, un message s'affiche sur le Bureau lorsque le FireWall rejette, c'est-à-dire bloque, une activité réseau d'une application.

Adresses IP bloquées

Si l'option est activée, un message s'affiche sur le Bureau lorsque le FireWall refuse le trafic de données d'une adresse IP.

Règles d'applications



Les options de la zone Règles d'applications vous permettent de régler les possibilités de configuration des règles d'applications sous la rubrique FireWall > Règles d'applications.

Paramètres avancés

Si l'option est activée, vous avez la possibilité de régler individuellement les différents accès réseau d'une application.

Réglages de base

Si l'option est activée, vous ne pouvez régler qu'une seule action pour les différents accès réseau de l'application.

Paramètres popup

Options disponibles uniquement si le mode expert est activé.

Paramètres popup

Inspecter la pile de lancement du processus

Si l'option est activée, une vérification plus précise de la pile de processus a lieu. Le FireWall part du principe que chaque processus suspect dans la pile est celui par lequel le processus enfant permet d'accéder au réseau. C'est pourquoi dans ce cas, une fenêtre popup s'ouvre pour chacun des processus suspects de la pile. Cette option est désactivée par défaut.

Afficher plusieurs boîtes de dialogue par processus

Si l'option est activée, une fenêtre popup s'ouvre à chaque fois qu'une application essaie d'établir une connexion au réseau. L'information peut également être donnée uniquement à la première tentative de connexion. Cette option est désactivée par défaut.

Enregistrer l'action pour cette application

Toujours activé

Si l'option est activée, l'option « **Enregistrer l'action pour cette application** » de la boîte de dialogue « **Événement réseau** » est activée par défaut.

Toujours désactivé

Si l'option est activée, l'option « **Enregistrer l'action pour cette application** » de la boîte de dialogue « **Événement réseau** » est désactivée par défaut.

Autoriser les applications signées

Si l'option est activée, l'option « **Enregistrer l'action pour cette application** » de la boîte de dialogue « **Événement réseau** » est activée automatiquement lors de l'accès au réseau d'applications signées de certains éditeurs. Ces applications signées sont

mises à disposition par des fournisseurs dignes de confiance (voir Fournisseurs dignes de confiance).

Mémoriser la dernière version utilisée

Si l'option est activée, l'activation de l'option « **Enregistrer l'action pour cette application** » de la boîte de dialogue « **Événement réseau** » est la même que lors du dernier événement réseau. Si l'option « **Enregistrer l'action pour cette application** » a été activée lors du dernier événement réseau, l'option est active pour l'événement réseau suivant. Si l'option « **Enregistrer l'action pour cette application** » a été désactivée lors du dernier événement réseau, l'option est désactivée pour l'événement réseau suivant.

Afficher les détails

Dans ce groupe d'options de configuration, vous pouvez paramétrer l'affichage des informations détaillées dans la fenêtre **Événement réseau**.

Afficher les détails sur demande

Si l'option est activée, les informations détaillées ne sont affichées dans la fenêtre « **Événement réseau** » que sur demande, c'est-à-dire que l'affichage des informations détaillées se fait en cliquant sur le bouton « **Afficher les détails** » dans la fenêtre **Événement réseau**.

Toujours afficher les détails

Si l'option est activée, les informations détaillées sont toujours affichées dans la fenêtre « **Événement réseau** ».

Mémoriser la dernière version utilisée

Si l'option est activée, l'affichage des informations détaillées est activé de la même manière que lors du précédent événement réseau. Si les informations détaillées ont été affichées lors du dernier événement réseau, elles le seront aussi lors de l'événement réseau suivant. Si les informations détaillées n'ont pas été affichées ou ont été masquées lors du dernier événement réseau, elles ne seront pas affichées lors de l'événement réseau suivant.

12.6 Protection Web

La rubrique **Protection Web** sous **Configuration > Sécurité Internet** sert à la configuration de la protection Web.

12.6.1 Recherche

La protection Web vous protège des virus et logiciels malveillants qui parviennent sur votre ordinateur par le biais des sites Internet que vous chargez dans votre navigateur Internet. Vous pouvez configurer le comportement de la protection Web dans la rubrique **Recherche**. (Options disponibles uniquement si le mode expert est activé.)

Recherche

Prise en charge IPv6

Si l'option est activée, la protection Web prend en charge la version 6 du protocole Internet. Cette option n'est pas disponible en cas de nouvelles installations ou modifiées sous Windows 8.

Protection contre les téléchargements automatiques intempestifs

La *protection contre les téléchargements automatiques intempestifs* vous permet de définir des paramètres visant à bloquer les I-Frames, appelées aussi Inline frames. Les I-Frames sont des éléments HTML, c'est-à-dire des éléments de sites Internet qui délimitent une zone d'une page Web. Grâce aux I-Frames, il est possible de charger et d'afficher d'autres contenus Web – le plus souvent d'autres URL – en tant que documents autonomes, dans une sous-fenêtre du navigateur. Les I-Frames sont la plupart du temps utilisées pour les bandeaux publicitaires. Dans certains cas, les I-Frames servent à dissimuler des logiciels malveillants. La zone de l'I-Frame n'est alors le plus souvent que peu ou pas visible dans le navigateur. L'option **Bloquer les I-Frames suspectes** vous permet de contrôler et de bloquer le chargement des I-Frames.

Bloquer les I-Frames suspectes

Si l'option est activée, les I-Frames des sites Internet demandés sont contrôlées selon certains critères. Si des I-Frames suspectes sont présentes sur un site Internet demandé, l'I-Frame est bloquée. Un message d'erreur s'affiche dans la fenêtre de l'I-Frame.

Action si résultat positif

Vous pouvez définir des actions que la protection Web doit exécuter quand un virus ou programme indésirable a été détecté. (Options disponibles uniquement si le mode expert est activé.)

Interactif

Si l'option est activée, une boîte de dialogue s'affiche dans laquelle vous pouvez sélectionner ce qui doit advenir du fichier contaminé en cas de détection d'un virus ou d'un programme indésirable pendant la recherche directe. Ce paramètre est activé par défaut.

Afficher la barre de progression

Si l'option est activée, un message affiché sur le Bureau apparaît avec une barre de progression de téléchargement, lorsque le téléchargement de contenus de sites Internet dépasse un délai d'attente de 20 secondes. Ce message affiché sur le Bureau sert notamment à contrôler le téléchargement de sites Internet avec de gros volumes de données : lors de la navigation avec la protection Web, les contenus des sites Internet ne sont pas chargés successivement dans le navigateur Internet, du fait qu'ils sont contrôlés quant à l'absence de virus et de logiciels malveillants avant d'être affichés dans le navigateur. Cette option est désactivée par défaut.

Vous trouverez de plus amples informations ici.

Automatique

Si l'option est activée, aucune boîte de dialogue permettant de sélectionner une action ne s'affiche en cas de détection d'un virus ou d'un programme indésirable. La protection Web réagit en fonction des paramètres réglés dans cette section.

Action primaire

L'action primaire est l'action exécutée lorsque la protection Web trouve un virus ou un programme indésirable.

Refuser l'accès

La page Web demandée par le serveur Web ou les données et fichiers transmis ne sont pas envoyés à votre navigateur Web. Un message d'erreur de refus d'accès s'affiche dans le navigateur Web. La protection Web inscrit le résultat positif dans le fichier rapport, dès lors que la fonction de rapport est activée.

Déplacer en quarantaine

La page Web demandée par le serveur Web ou les données et fichiers transmis sont déplacés en quarantaine en cas de détection d'un virus ou d'un logiciel malveillant. Le fichier concerné peut être restauré depuis le gestionnaire de quarantaines s'il a une valeur informative ou, si nécessaire, être envoyé à l'Avira Malware Research Center.

Ignorer

La page Web demandée par le serveur Web ou les données et fichiers transmis sont envoyés à votre navigateur Web par la protection Web. L'accès au fichier est autorisé et le fichier est conservé.

Avertissement
Le fichier contaminé reste actif sur votre ordinateur. D'importants dégâts peuvent être causés sur votre ordinateur.

Accès bloqués

Sous **Accès bloqués**, vous pouvez indiquer les types de fichiers et les types MIME (types de contenus des données transmises) qui doivent être bloqués par la protection Web. Le filtre Web vous permet de bloquer les URL indésirables et connues, comme par ex. des URL de hameçonnage et de logiciel malveillant. La protection Web empêche la transmission des données depuis Internet vers votre ordinateur. (Options disponibles uniquement si le mode expert est activé.)

Types de fichiers / types MIME bloqués par la protection Web

Tous les types de fichiers et les types MIME (types de contenus des données transmises) figurant dans la liste sont bloqués par la protection Web.

Champ de saisie

Saisissez dans ce champ les noms des types MIME et des types de fichiers qui doivent être bloqués par la protection Web. Pour les types de fichiers, saisissez l'extension de fichier, par ex. **.htm**. Pour les types MIME, notez le type de support et éventuellement le sous-type. Les deux indications sont séparées par une barre oblique, par ex. **video/mpeg** ou **audio/x-wav**.

> **Remarque**
> Les fichiers qui ont déjà été enregistrés sur votre ordinateur comme fichiers Internet temporaires sont certes bloqués par la protection Web, mais peuvent être chargés localement par votre ordinateur à partir du navigateur Internet. Les fichiers Internet temporaires sont des fichiers sauvegardés sur votre ordinateur par le navigateur Internet, pour pouvoir afficher plus rapidement les sites Internet.

> **Remarque**
> La liste des types de fichiers et types MIME à bloquer est ignorée pour les entrées figurant dans la liste des types de fichiers et types MIME à exclure sous Exceptions.

> **Remarque**
> Lorsque vous indiquez des types de fichiers et des types MIME, vous ne pouvez pas utiliser de caractères de remplacement (caractère de remplacement * pour un nombre quelconque de caractères ou ? pour un caractère exactement).

Types MIME : exemples de types de supports

- `text` = pour fichiers texte
- `image` = pour fichiers graphiques
- `video` = pour fichiers vidéo
- `audio` = pour fichiers son
- `application` = pour les fichiers associés à un programme particulier

Exemples : types de fichiers et types MIME à exclure

- `application/octet-stream` = les fichiers du type MIME application/octet-stream (fichiers exécutables *.bin, *.exe, *.com, *dll, *.class) sont bloqués par la protection Web.
- `application/olescript` = les fichiers du type MIME application/olescript (fichiers script ActiveX *.axs) sont bloqués par la protection Web.

- `.exe` = tous les fichiers avec l'extension .exe (fichiers exécutables) sont bloqués par la protection Web.
- `.msi` = tous les fichiers avec l'extension .msi (fichiers Windows Installer) sont bloqués par la protection Web.

Ajouter

Ce bouton vous permet de valider dans la fenêtre d'affichage le type MIME ou de fichier entré dans le champ de saisie.

Supprimer

Le bouton supprime une entrée sélectionnée de la liste. Ce bouton n'est pas actif si aucune entrée n'est sélectionnée.

Filtre Web

Le filtre Web dispose d'une base de données interne mise à jour quotidiennement, dans laquelle les URL sont classées par critères de contenus.

Activer le filtre Web

Si l'option est activée, toutes les URL figurant parmi les catégories sélectionnées dans la liste du filtre Web sont bloquées.

Liste du filtre Web

La liste du filtre Web vous permet de choisir les catégories de contenus dont les URL doivent être bloquées par la protection Web.

> **Remarque**
> Le filtre Web est ignoré pour les entrées figurant dans la liste des URL à ignorer sous Exceptions.

> **Remarque**
> La rubrique **URL de spam** reprend les URL diffusées par des e-mails de spam. La catégorie **Arnaque / fraude** englobe les sites Internet comportant des « pièges d'abonnement » et autres offres de services dont les coûts sont dissimulés par le fournisseur.

Exceptions

Ces options vous permettent d'exclure des types MIME (types de contenus des données transmises) et des types de fichiers d'URL (adresses Internet) de la recherche effectuée par la protection Web. Les types MIME et les URL indiqués sont ignorés par la protection Web, ce qui signifie que ces données ne sont pas contrôlées quant à l'absence de virus et

logiciels malveillants, lors de la transmission sur votre ordinateur. (Options disponibles uniquement si le mode expert est activé.)

Types MIME à exclure par la protection Web

Dans ce champ, vous pouvez sélectionner les types MIME (types de contenus des données transmises) à exclure de la recherche par la protection Web.

Types de fichiers / types MIME à exclure par la protection Web (définis par l'utilisateur)

Tous les types de fichiers et types MIME (types de contenus des données transmises) figurant dans la liste sont exclus de la recherche par la protection Web.

Champ de saisie

Dans ce champ, vous pouvez indiquer les noms des types MIME et des types de fichiers à exclure de la recherche par la protection Web. Pour les types de fichiers, saisissez l'extension de fichier, par ex. `.htm`. Pour les types MIME, notez le type de support et éventuellement le sous-type. Les deux indications sont séparées par une barre oblique, par ex. `video/mpeg` ou `audio/x-wav`.

Remarque
Lorsque vous indiquez des types de fichiers et des types MIME, vous ne pouvez pas utiliser de caractères de remplacement (caractère de remplacement * pour un nombre quelconque de caractères ou ? pour un caractère exactement).

Avertissement
Tous les types de fichiers et de contenus figurant sur la liste d'exclusion sont chargés dans le navigateur Internet sans contrôle additionnel des accès bloqués (liste des types fichiers et types MIME à bloquer sous Accès bloqués) ou de la protection Web : pour toutes les entrées figurant sur la liste d'exclusion, les entrées de la liste des types de fichiers et types MIME à bloquer sont ignorées. Aucune recherche de virus et de logiciels malveillants n'est effectuée.

Types MIME : exemples de types de supports

- `text` = pour fichiers texte
- `image` = pour fichiers graphiques
- `video` = pour fichiers vidéo
- `audio` = pour fichiers son
- `application` = pour les fichiers associés à un programme particulier

Exemples : types de fichiers et types MIME à exclure



- `audio/` = tous les fichiers de type audio sont exclus de la recherche effectuée par la protection Web
- `video/quicktime` = tous les fichiers vidéo du sous-type Quicktime (*.qt, *.mov) sont exclus de la recherche effectuée par la protection Web
- `.pdf` = tous les fichiers PDF Adobe sont exclus de la recherche effectuée par la protection Web.

Ajouter

Ce bouton vous permet de valider dans la fenêtre d'affichage le type MIME ou de fichier entré dans le champ de saisie.

Supprimer

Le bouton supprime une entrée sélectionnée de la liste. Ce bouton n'est pas actif si aucune entrée n'est sélectionnée.

URL à exclure par la protection Web

Toutes les URL de cette liste sont exclues de la recherche effectuée par la protection Web.

Champ de saisie

Saisissez dans ce champ les URL (adresses Internet) à exclure de la recherche par la protection Web, par ex. **www.nomdedomaine.com**. Vous pouvez indiquer des parties de l'URL en signalant le niveau de domaine avec des points finaux ou de début : nomdedomaine.fr pour tous les sites et tous les sous-domaines du domaine. Notez un site Web avec un domaine de niveau supérieur quelconque (.com ou .net) avec un point final : **nomdedomaine.**. Si vous notez une suite de caractères sans point final ou point de début, celle-ci sera interprétée comme un domaine de niveau supérieur, par ex. **net** pour tous les domaines NET (www.domaine.net).

Remarque
Lors de l'indication des URL, vous pouvez également utiliser le caractère de remplacement * pour un nombre quelconque de caractères. Utilisez aussi des points finaux ou de début en combinaison avec les caractères de remplacement, pour repérer les niveaux de domaine :
`nomdedomaine.*`
`*.nomdedomaine.com`
`.*nom*.com` (applicable mais pas recommandé)
Les indications sans points comme `*nom*` sont interprétées comme des parties d'un domaine de niveau supérieur et ne sont donc pas judicieuses.

Avertissement
Tous les sites Web figurant sur la liste des URL à exclure sont chargés dans le navigateur Internet sans contrôle additionnel de la part du filtre Web ou de la

protection Web : pour toutes les entrées figurant dans la liste des URL à exclure, les entrées du filtre Web sont ignorées (voir Accès bloqués). Aucune recherche de virus et de logiciels malveillants n'est effectuée. Par conséquent, n'excluez de la recherche par la protection Web que les URL dignes de confiance.

Ajouter

Ce bouton vous permet de valider dans la fenêtre d'affichage l'URL (adresse Internet) entrée dans le champ de saisie.

Supprimer

Le bouton supprime une entrée sélectionnée de la liste. Ce bouton n'est pas actif si aucune entrée n'est sélectionnée.

Exemples : URL à exclure

- `www.avira.com` -OU- `www.avira.com/*`
  = toutes les URL avec le domaine www.avira.com sont exclues de la recherche effectuée par la protection Web : www.avira.com/en/pages/index.php, www.avira.com/en/support/index.html, www.avira.com/en/download/index.html,...
  Les URL avec le domaine www.avira.fr ne sont pas exclues de la recherche effectuée par la protection Web.
- `avira.com` -OU- `*.avira.com`
  = toutes les URL avec le domaine de second niveau et de niveau supérieur avira.com sont exclues de la recherche effectuée par la protection Web. L'indication implique tous les sous-domaines existants pour .avira.com : www.avira.com, forum.avira.com,...
- `avira.` -OU- `*.avira.*`
  = toutes les URL avec le domaine de second niveau avira sont exclues de la recherche effectuée par la protection Web. L'indication implique tous les domaines de niveau supérieur ou les sous-domaines existants pour .avira. : www.avira.com, www.avira.fr, forum.avira.com,...
- `.*domain*.*`
  = toutes les URL contenant un domaine de second niveau avec la chaîne de caractères domain sont exclues de la recherche effectuée par la protection Web : www.domain.com, www.new-domain.fr, www.sample-domain1.fr, ...
- `net` -OU- `*.net`
  = toutes les URL avec le domaine de niveau supérieur net sont exclues de la recherche effectuée par la protection Web : www.name1.net, www.name2.net,...

Avertissement
Indiquez aussi précisément que possible les URL que vous souhaitez exclure de la recherche effectuée par la protection Web. Évitez d'indiquer des ensembles de domaines de niveau supérieur ou des parties d'un nom de domaine de second niveau, car il y a un risque que des pages Internet

propageant des logiciels malveillants ou programmes indésirables soient exclues de la recherche effectuée par la protection Web par des indications globales définies sous la rubrique Exceptions. Il est recommandé d'indiquer au moins le domaine de second niveau entièrement et le domaine de niveau supérieur : nomdedomaine.com

Heuristique

Cette rubrique de configuration contient les paramètres pour l'heuristique du moteur de recherche. (Options disponibles uniquement si le mode expert est activé.)

Les produits Avira contiennent des heuristiques très performantes qui permettent de détecter dynamiquement des logiciels malveillants inconnus, c'est-à-dire avant même qu'une signature de virus spéciale n'ait été créée contre le parasite et qu'une mise à jour de protection antivirus correspondante n'ait été envoyée. La détection des virus s'effectue par une analyse complexe et un examen du code en cause, à la recherche de fonctions typiques des logiciels malveillants. Si le code examiné présente ces caractéristiques, il est signalé comme suspect. Cela ne signifie pas obligatoirement que le code est un logiciel malveillant ; des messages erronés peuvent aussi survenir. C'est l'utilisateur qui doit décider comment traiter le code, par ex. sur la base de ses connaissances pour savoir si la source contenant le code signalé est digne de confiance.

Heuristique de macrovirus

Votre produit Avira contient une heuristique de macrovirus très performante. Si l'option est activée, toutes les macros du document contaminé sont supprimées si une réparation est possible ; les documents suspects peuvent aussi être seulement signalés, c'est-à-dire que vous recevez un avertissement. Ce paramètre est activé par défaut et recommandé.

Advanced Heuristic Analysis and Detection (AHeAD)

Activer AHeAD

Votre produit Avira contient une heuristique très performante grâce à la technologie Avira AHeAD, lui permettant de détecter aussi les (nouveaux) logiciels malveillants inconnus. Si l'option est activée, vous pouvez régler ici la sensibilité de cette heuristique. Ce paramètre est activé par défaut.

Niveau de détection bas

Si l'option est activée, moins de logiciels malveillants inconnus sont détectés, le risque de détections erronées est faible dans ce cas.

Niveau de détection moyen

Si l'option est activée, une protection équilibrée est assurée avec peu de messages d'erreurs. Ce paramètre est activé par défaut si vous avez choisi l'utilisation de cette heuristique.

Niveau de détection élevé

Si l'option est activée, nettement plus de logiciels malveillants inconnus sont détectés, sachant qu'il faut toutefois s'attendre à des messages erronés.

12.6.2 Rapport

La protection Web dispose d'une fonction étendue de consignation qui peut donner à l'utilisateur et à l'administrateur des indications exactes sur un résultat positif.

Consignation

Ce groupe permet de définir le contenu du fichier rapport.

Désactivée

Si l'option est activée, la protection Web ne génère pas de rapport.
Ne renoncez à la consignation que dans des cas exceptionnels, par ex. uniquement lorsque vous effectuez des tests avec de nombreux virus ou programmes indésirables.

Par défaut

Si l'option est activée, la protection Web consigne les informations importantes (sur les résultats positifs, les avertissements et les erreurs) dans le fichier rapport, les informations secondaires sont ignorées pour une meilleure lisibilité. Ce paramètre est activé par défaut.

Étendue

Si l'option est activée, la protection Web consigne également les informations secondaires dans le fichier rapport.

Intégrale

Si cette option est activée, la protection Web consigne toutes les informations dans le fichier rapport, même celles sur la taille et le type des fichiers, la date, etc.

Limiter le fichier rapport

Limiter la taille à n Mo

Si l'option est activée, il est possible de limiter la taille du fichier rapport ; valeurs possibles : 1 à 100 Mo. En cas de limitation du fichier rapport, une marge d'environ 50 kilo-octets est laissée pour ne pas trop solliciter l'ordinateur. Si la taille du fichier rapport dépasse la taille indiquée de 50 kilo-octets, les anciennes entrées sont supprimées automatiquement jusqu'à ce que la taille indiquée moins 20 % soit atteinte.

Écrire la configuration dans le fichier rapport

Si l'option est activée, la configuration de la recherche en temps réel utilisée est écrite dans le fichier rapport.

Remarque
Si vous n'avez indiqué aucune limitation du fichier rapport, les anciennes entrées sont automatiquement supprimées lorsque le fichier rapport a atteint une taille de 100 Mo. Les entrées sont supprimées tant que le fichier rapport n'a pas atteint une taille de 80 Mo.

12.7 Protection e-mail

La rubrique Protection e-mail de la configuration permet de configurer la protection e-mail.

12.7.1 Recherche

Vous utilisez la protection e-mail pour contrôler les e-mails entrants quant à l'absence de virus, de logiciels malveillants et de spam. Il est possible de faire contrôler les e-mails sortants par la protection e-mail quant à l'absence de virus et de logiciels malveillants. La protection e-mail peut bloquer les e-mails sortants qui sont envoyés sur votre ordinateur par un bot inconnu pour diffuser des spams.

Contrôler les e-mails entrants

Si l'option est activée, les e-mails entrants sont contrôlés quant à l'absence de virus, de logiciels malveillants et de spam. La protection e-mail prend en charge les protocoles POP3 et IMAP. Activez le compte de la boîte de réception utilisé par votre client de messagerie pour la réception des e-mails, pour le faire surveiller par la protection e-mail.

Surveiller les comptes POP3

Si l'option est activée, les comptes POP3 sont surveillés sur les ports indiqués.

Ports surveillés

Saisissez dans ce champ le port utilisé comme boîte de réception par le protocole POP3. Vous pouvez indiquer plusieurs ports en les séparant par des virgules. (Option disponible uniquement si le mode expert est activé.)

Par défaut

Ce bouton permet de réinitialiser les ports indiqués au port POP3 par défaut. (Option disponible uniquement si le mode expert est activé.)

Surveiller les comptes IMAP

Si l'option est activée, les comptes IMAP sont surveillés sur les ports indiqués.

Ports surveillés

Saisissez dans ce champ le port utilisé par le protocole IMAP. Vous pouvez indiquer plusieurs ports en les séparant par des virgules. (Option disponible uniquement si le mode expert est activé.)



Par défaut

Ce bouton permet de réinitialiser les ports indiqués au port IMAP par défaut. (Option disponible uniquement si le mode expert est activé.)

Contrôler les e-mails sortants (SMTP)

Si l'option est activée, les e-mails sortants sont contrôlés quant à l'absence de virus et de logiciels malveillants. Les e-mails envoyés par des bots inconnus pour diffuser des spams sont bloqués.

Ports surveillés

Saisissez dans ce champ le port utilisé comme boîte d'envoi par le protocole SMTP. Vous pouvez indiquer plusieurs ports en les séparant par des virgules. (Option disponible uniquement si le mode expert est activé.)

Par défaut

Ce bouton permet de réinitialiser les ports indiqués au port SMTP par défaut. (Option disponible uniquement si le mode expert est activé.)

Remarque
Pour vérifier les protocoles et les ports utilisés, consultez les propriétés de vos comptes dans votre programme client de messagerie électronique. Les ports par défaut sont ceux qui sont utilisés par la majorité des comptes de messagerie.

Prise en charge IPv6

Si l'option est activée, la protection e-mail prend en charge la version 6 du protocole Internet. (Option disponible uniquement si le mode expert est activé et non en cas de nouvelles installations ou modifiées sous Windows 8.)

Action si résultat positif

Cette rubrique de configuration contient des paramètres concernant les actions effectuées lorsque la protection e-mail trouve un virus ou un programme indésirable dans un e-mail ou une pièce jointe. (Options disponibles uniquement si le mode expert est activé.)

Remarque
Les actions définies ici sont exécutées en cas de détection de virus dans des e-mails entrants, de même que dans des e-mails sortants.

Interactif

Si l'option est activée, une boîte de dialogue s'affiche pour sélectionner l'action à effectuer avec le fichier contaminé ou la pièce jointe en cas de détection d'un virus ou d'un programme indésirable dans un e-mail ou une pièce jointe. Cette option est activée par défaut.



Afficher la barre de progression

Si l'option est activée, la protection e-mail affiche une barre de progression pendant le téléchargement des e-mails. L'activation de cette option n'est possible que si l'option **Interactif** a été sélectionnée.

Automatique

Si l'option est activée, vous n'êtes plus prévenu si un virus ou un programme indésirable est détecté. La protection e-mail réagit en fonction des paramètres définis dans cette section.

E-mails contaminés

L'option choisie sous « *E-mails contaminés* » est exécutée en tant qu'action primaire si la protection e-mail trouve un virus ou un programme indésirable dans un e-mail. Si l'option « **Ignorer** » est sélectionnée, vous pouvez choisir sous « *Pièces jointes contaminées* **»** ce qui doit se passer quand un résultat positif est détecté dans une pièce jointe.

Supprimer

Si cette option est activée, l'e-mail contaminé est automatiquement supprimé si un virus ou un programme indésirable a été détecté. Le corps de l'e-mail (body) est remplacé par le texte standard ci-dessous. La même chose s'applique à toutes les pièces jointes (attachments) ; celles-ci sont également remplacées par un texte standard.

Ignorer

Si l'option est activée, l'e-mail contaminé est ignoré même si un virus ou un programme indésirable a été détecté. Vous avez toutefois la possibilité de décider ce qui doit advenir d'une pièce jointe contaminée.

Déplacer en quarantaine

Si l'option est activée, l'e-mail complet avec toutes ses pièces jointes est mis en Quarantaine si un virus ou un programme indésirable est détecté. Il peut être restauré ensuite sur demande. L'e-mail contaminé lui-même est supprimé. Le corps de l'e-mail (body) est remplacé par le texte standard ci-dessous. La même chose s'applique à toutes les pièces jointes (attachments) ; celles-ci sont également remplacées par un texte standard.

Pièces jointes contaminées

L'option « **Pièces jointes contaminées** » ne peut être sélectionnée que si, sous « *E-mails contaminés* **»**, l'option « **Ignorer** » a été sélectionnée. Cette option permet de décider ce qui doit être fait si une pièce jointe est contaminée.

Supprimer

Si l'option est activée, la pièce jointe contaminée par un virus ou un programme indésirable est supprimée et remplacée par un texte standard.

Ignorer

Si l'option est activée, la pièce jointe contaminée est ignorée et délivrée même si un virus ou un programme indésirable a été détecté.

Avertissement
Si vous choisissez cette option, vous n'êtes pas du tout protégé des virus et programmes indésirables par la protection e-mail. Ne choisissez cette rubrique que si vous savez exactement ce que vous faites. Désactivez l'aperçu dans votre programme de messagerie électronique, n'ouvrez pas les pièces jointes par double-clic.

Déplacer en quarantaine

Si cette option est activée, la pièce jointe contaminée est placée en quarantaine puis supprimée (remplacée par un texte standard). La pièce jointe contaminée peut être restaurée ensuite, sur demande.

Autres actions

Cette rubrique de configuration contient d'autres paramètres concernant les actions effectuées lorsque la protection e-mail trouve un virus ou un programme indésirable dans un e-mail ou une pièce jointe. (Options disponibles uniquement si le mode expert est activé.)

Remarque
Les actions définies ici sont exécutées exclusivement en cas de détection de virus dans des e-mails entrants.

Texte standard pour les e-mails supprimés et déplacés

Le texte dans ce champ est ajouté comme message dans l'e-mail, à la place de l'e-mail contaminé. Vous pouvez modifier ce message. Un texte ne doit pas contenir plus de 500 caractères.

Vous pouvez utiliser les combinaisons de touches suivantes pour la mise en forme :

Ctrl + Enter = ajoute un saut de ligne.

Par défaut

Le bouton insère un texte standard prédéfini dans le champ d'édition.

Texte standard pour les pièces jointes supprimées et déplacées

Le texte de ce champ est ajouté comme message dans l'e-mail, à la place de la pièce jointe contaminée. Vous pouvez modifier ce message. Un texte ne doit pas contenir plus de 500 caractères.

Vous pouvez utiliser les combinaisons de touches suivantes pour la mise en forme :



Ctrl + Enter = ajoute un saut de ligne.

Par défaut

Le bouton insère un texte standard prédéfini dans le champ d'édition.

Heuristique

Cette rubrique de configuration contient les paramètres pour l'heuristique du moteur de recherche. (Options disponibles uniquement si le mode expert est activé.)

Les produits Avira contiennent des heuristiques très performantes qui permettent de détecter dynamiquement des logiciels malveillants inconnus, c'est-à-dire avant même qu'une signature de virus spéciale n'ait été créée contre le parasite et qu'une mise à jour de protection antivirus correspondante n'ait été envoyée. La détection des virus s'effectue par une analyse complexe et un examen du code en cause, à la recherche de fonctions typiques des logiciels malveillants. Si le code examiné présente ces caractéristiques, il est signalé comme suspect. Cela ne signifie pas obligatoirement que le code est un logiciel malveillant ; des messages erronés peuvent aussi survenir. C'est l'utilisateur qui doit décider comment traiter le code, par ex. sur la base de ses connaissances pour savoir si la source contenant le code signalé est digne de confiance.

Heuristique de macrovirus

Votre produit Avira contient une heuristique de macrovirus très performante. Si l'option est activée, toutes les macros du document contaminé sont supprimées si une réparation est possible ; les documents suspects peuvent aussi être seulement signalés, c'est-à-dire que vous recevez un avertissement. Ce paramètre est activé par défaut et recommandé.

Advanced Heuristic Analysis and Detection (AHeAD)

Activer AHeAD

Votre produit Avira contient une heuristique très performante grâce à la technologie Avira AHeAD, lui permettant de détecter aussi les (nouveaux) logiciels malveillants inconnus. Si l'option est activée, vous pouvez régler ici la sensibilité de cette heuristique. Ce paramètre est activé par défaut.

Niveau de détection bas

Si l'option est activée, moins de logiciels malveillants inconnus sont détectés, le risque de détections erronées est faible dans ce cas.

Niveau de détection moyen

Si l'option est activée, une protection équilibrée est assurée avec peu de messages d'erreurs. Ce paramètre est activé par défaut si vous avez choisi l'utilisation de cette heuristique.

Niveau de détection élevé

Si l'option est activée, nettement plus de logiciels malveillants inconnus sont détectés, sachant qu'il faut toutefois s'attendre à des messages erronés.



AntiBot

La fonction AntiBot de la protection e-mail vous permet d'empêcher que votre ordinateur ne soit utilisé comme partie d'un réseau bot pour distribuer des spams : lors de la diffusion de spam par un réseau bot, l'agresseur infecte en règle générale plusieurs ordinateurs avec un bot qui se connecte ensuite à un serveur IRC, entre dans un canal particulier et de là, attend de recevoir l'ordre d'envoyer des spams. Pour différencier les spams d'un bot inconnu des e-mails de l'utilisateur de l'ordinateur, la protection e-mail vérifie si le serveur SMTP utilisé et l'expéditeur d'un e-mail sortant sont bien mentionnés dans les listes des serveurs et expéditeurs autorisés. Si ce n'est pas le cas, l'e-mail sortant est bloqué, c'est-à-dire que l'e-mail n'est pas envoyé. L'e-mail bloqué est signalé dans une fenêtre de dialogue. (Options disponibles uniquement si le mode expert est activé.)

> **Remarque**
> La fonction AntiBot ne peut être utilisée que si la recherche de la protection e-mail est active pour les e-mails sortants (voir option **Contrôler les e-mails sortants** sous Protection e-mail > Recherche).

Serveurs autorisés

Tous les serveurs figurant dans la liste sont autorisés par la protection e-mail pour l'envoi d'e-mail : les e-mails envoyés à ces serveurs ne sont **pas** bloqués par la protection e-mail. Si aucun serveur n'est indiqué dans la liste, aucune vérification du serveur SMTP utilisé n'est effectuée pour les e-mails sortants. Si la liste contient des entrées, la protection e-mail bloque les e-mails qui sont envoyés à un serveur SMTP ne figurant pas sur la liste.

Champ de saisie

Saisissez dans ce champ le nom d'hôte ou l'adresse IP du serveur SMTP que vous utilisez pour envoyer vos e-mails.

> **Remarque**
> Vous trouverez les informations concernant les serveurs SMTP utilisés par votre programme de messagerie pour l'envoi d'e-mails dans les données de votre programme sur les comptes utilisateurs créés.

Ajouter

Ce bouton vous permet d'ajouter les serveurs indiqués dans le champ de saisie à la liste des serveurs autorisés.

Supprimer

Ce bouton efface une entrée sélectionnée dans la liste des serveurs autorisés. Ce bouton n'est pas actif si aucune entrée n'est sélectionnée.



Tout supprimer

Ce bouton supprime toutes les entrées de la liste des serveurs autorisés.

Expéditeurs autorisés

Tous les expéditeurs figurant dans cette liste sont autorisés par la protection e-mail pour l'envoi d'e-mails : les e-mails envoyés depuis cette adresse e-mail ne sont **pas** bloqués par la protection e-mail. Si aucun expéditeur n'est mentionné dans la liste, aucune vérification de l'adresse e-mail utilisée par l'expéditeur n'est effectuée pour les e-mails sortants. Si la liste contient des entrées, la protection e-mail bloque les e-mails des expéditeurs ne figurant pas sur la liste.

Champ de saisie

Saisissez dans ce champ votre/vos adresse(s) e-mail d'expéditeur.

Ajouter

Ce bouton vous permet d'ajouter les expéditeurs indiqués dans le champ de saisie à la liste des expéditeurs autorisés.

Supprimer

Ce bouton supprime une entrée sélectionnée dans la liste des expéditeurs autorisés. Ce bouton n'est pas actif si aucune entrée n'est sélectionnée.

Tout supprimer

Ce bouton supprime toutes les entrées de la liste des expéditeurs autorisés.

12.7.2 Généralités

Exceptions

Adresses e-mail qui ne sont pas contrôlées

Ce tableau vous donne la liste des adresses e-mail qui ont été exclues du contrôle effectué par la protection e-mail d'Avira (liste blanche).

> **Remarque**
> La liste des exceptions est utilisée par la protection e-mail exclusivement pour les e-mails entrants.

Adresses e-mail qui ne sont pas contrôlées

Champ de saisie

Saisissez dans ce champ l'adresse e-mail que vous souhaitez ajouter à la liste des adresses e-mail à ne pas contrôler. L'adresse e-mail ne sera dorénavant plus contrôlée par la protection e-mail, en fonction de vos paramètres.

Remarque
Lorsque vous saisissez des adresses e-mail, vous pouvez utiliser de caractères de remplacement : caractère de remplacement ***** pour un nombre quelconque de caractères ou **?** pour un caractère exactement. Les caractères de remplacement ne peuvent toutefois être utilisés que pour les adresses e-mail qui ne doivent pas être contrôlées quant à l'absence de spam. Vous recevez donc un message d'erreur quand vous tentez d'exclure une adresse contenant des caractères de remplacement du contrôle concernant l'absence de logiciels malveillants, en activant la case à cocher **Logiciels malveillants** dans la liste d'exclusions. Lors de la saisie d'adresses avec des caractères de remplacement, tenez compte du fait que la série de caractères indiquée doit correspondre à la structure d'une adresse e-mail (*@*.*).

Avertissement
Tenez compte des exemples donnés lors de l'utilisation de caractères de remplacement. N'utilisez les caractères de remplacement que de manière ciblée et contrôlez précisément les adresses e-mail que vous acceptez dans la liste blanche de spam en saisissant des caractères de remplacement.

Exemples : utilisation de caractères de remplacement dans les adresses e-mail (liste blanche de spam)

- `virus@avira.* /` = comprend tous les e-mails avec cette adresse et n'importe quel domaine de niveau supérieur : virus@avira.fr, virus@avira.com, virus@avira.net,...
- `*@avira.com` = comprend tous les e-mails envoyés à partir du domaine **avira.com** : info@avira.com, virus@avira.com, contact@avira.com, employé@avira.com
- `info@*.com` = comprend toutes les adresses e-mail avec le domaine de niveau supérieur **com** et l'adresse **info** ; le domaine de second niveau peut être n'importe lequel : info@name1.com, info@name2.com,...

Ajouter

Ce bouton vous permet d'ajouter à la liste des adresses e-mail à ne pas contrôler l'adresse e-mail entrée dans le champ de saisie.

Supprimer

Ce bouton supprime l'adresse e-mail sélectionnée dans la liste.



Adresse e-mail

Adresse e-mail qui ne doit plus être contrôlée.

Logiciels malveillants

Si l'option est activée, l'adresse e-mail ne sera plus contrôlée quant à la présence de logiciels malveillants.

Spam

Si l'option est activée, l'adresse e-mail ne sera plus contrôlée quant à la présence de spams.

vers le haut

Ce bouton vous permet de déplacer une adresse e-mail sélectionnée d'une position vers le haut. Ce bouton n'est pas disponible si aucune entrée n'est sélectionnée ou si l'adresse sélectionnée figure en première position dans la liste.

vers le bas

Ce bouton vous permet de déplacer une adresse e-mail sélectionnée d'une position vers le bas. Ce bouton n'est pas disponible si aucune entrée n'est sélectionnée ou si l'adresse sélectionnée figure en dernière position dans la liste.

Importer le carnet d'adresses Outlook

Ce bouton vous permet d'importer les adresses e-mail du carnet d'adresses du programme de messagerie MS Outlook dans la liste des exceptions. Les adresses e-mail importées ne sont pas contrôlées quant à la présence de spam.

Importer le carnet d'adresses Outlook Express (Windows XP) / Importer le carnet d'adresses Windows Mail (Windows Vista, Windows 7)

Ce bouton vous permet d'importer les adresses e-mail du carnet d'adresses du programme de messagerie MS Outlook Express ou Windows Mail dans la liste des exceptions. Les adresses e-mail importées ne sont pas contrôlées quant à la présence de spam.

Mémoire tampon

La mémoire tampon de la protection e-mail contient les données sur les e-mails contrôlés qui sont affichés dans les statistiques du Control Center sous **Protection e-mail**. (Options disponibles uniquement si le mode expert est activé.)

En outre, des copies des e-mails entrants sont stockées dans la mémoire tampon. Les e-mails sont utilisés pour les fonctions d'apprentissage (*E-mail normal – utiliser pour l'apprentissage*, *Spam – utiliser pour l'apprentissage*) du module AntiSpam.

> **Remarque**
> Pour que les e-mails entrants soient enregistrés dans la mémoire tampon, le module AntiSpam doit être activé.

Nombre maximum d'e-mails dans la mémoire tampon

Saisissez dans ce champ le nombre maximum d'e-mails conservés dans la mémoire tampon de la protection e-mail. Les e-mails les plus anciens sont supprimés.

Durée de mémorisation maximale d'un e-mail en jours

Saisissez dans ce champ la durée de mémorisation maximale d'un e-mail en jours. Après cet intervalle, l'e-mail est supprimé de la mémoire tampon.

Vider la mémoire tampon

Cliquez sur ce bouton pour supprimer les e-mails conservés dans la mémoire tampon.

Pied de page

Sous **Pied de page**, vous pouvez configurer un pied de page qui sera affiché dans les e-mails que vous envoyez. (Options disponibles uniquement si le mode expert est activé.)

Pour cette fonction, il est indispensable d'activer le contrôle de la protection e-mail pour les e-mails sortants ; voir option **Contrôler les e-mails sortants (SMTP)** sous **Configuration > Protection e-mail > Recherche**. Vous pouvez utiliser le pied de page défini de la protection e-mail d'Avira avec lequel vous confirmez que l'e-mail envoyé a été contrôlé par un programme de protection anti-virus. Vous avez également la possibilité d'entrer un texte afin de créer un pied de page personnalisé. Si vous utilisez les deux options pour le pied de page, le texte personnalisé précède le pied de page de la protection e-mail d'Avira.

Pied de page pour les e-mails à envoyer

Joindre le pied de page de la protection e-mail

Si l'option est activée, le pied de page de la protection e-mail d'Avira est affiché sous le texte du message des e-mails envoyés. Avec le pied de page de la protection e-mail d'Avira, vous confirmez que l'e-mail envoyé a été contrôlé par la protection e-mail d'Avira quant à la présence de virus et de programmes indésirables et qu'il ne provient pas d'un bot inconnu. Le pied de page de la protection e-mail d'Avira contient le texte suivant : « *Contrôlé avec la protection e-mail d'Avira [version de produit] [abréviation du nom et numéro de version du moteur de recherche] [abréviation du nom et numéro de version du fichier de définitions des virus]* ».

Joindre ce pied de page

Si l'option est activée, le texte que vous indiquez dans le champ de saisie s'affiche en pied de page dans les e-mails envoyés.



Champ de saisie

Dans ce champ de saisie, vous pouvez entrer un texte qui sera affiché en pied de page dans les e-mails envoyés.

AntiSpam

La protection e-mail d'Avira contrôle l'absence de virus et de programmes indésirables dans les e-mails. En outre, elle peut vous protéger efficacement contre les spams. (Options disponibles uniquement si le mode expert est activé.)

Activer le module AntiSpam

Si l'option est activée, la fonction AntiSpam de la protection e-mail est activée.

Marquer l'objet de l'e-mail

Si l'option est activée, une mention est ajoutée à l'objet d'origine si l'e-mail est identifié comme spam.

Simple

Une mention supplémentaire [SPAM] ou [Phishing] est ajoutée à l'objet si l'e-mail est un spam ou un e-mail de hameçonnage. Cette option est activée par défaut.

Détaillé

Une mention étendue indiquant la probabilité qu'il s'agisse d'un spam est ajoutée à l'objet de l'e-mail de spam ou de hameçonnage.

Consigner

Si l'option est activée, la protection e-mail génère un fichier rapport spécial AntiSpam.

Utiliser les listes noires en temps réel (RBL)

Si l'option est activée, une liste noire est interrogée en temps réel. Elle contient des informations supplémentaires pour classer les e-mails d'origine douteuse comme spams.

Délai d'attente : n seconde(s)

Si les informations d'une liste noire ne sont pas disponibles au bout de n secondes, la tentative d'accès à la liste noire est interrompue.

Supprimer la base de données d'apprentissage

La base de données d'apprentissage est effacée si vous cliquez sur ce bouton.

Ajouter automatiquement les destinataires des e-mails sortants à la liste blanche

Si l'option est activée, les adresses des destinataires d'e-mails sortants sont reprises automatiquement dans la liste blanche de spam (liste des e-mails qui ne doivent pas être contrôlés quant à l'absence de spam sous **Protection e-mail > Généralités > Exceptions**). Les e-mails entrants qui sont envoyés à partir des adresses de la liste

blanche de spam ne sont pas contrôlés quant à l'absence de spam. Le contrôle concernant les virus et logiciels malveillants continue d'être effectué. Cette option est désactivée par défaut.

> **Remarque**
> Cette option ne peut être activée que si la recherche de la protection e-mail est active pour les e-mails sortants (voir option **Contrôler les e-mails sortants** sous Protection e-mail > Recherche).

12.7.3 Rapport

La protection e-mail dispose d'une fonction étendue de consignation qui peut donner à l'utilisateur et à l'administrateur des indications exactes sur un résultat positif.

Consignation

Ce groupe permet de définir le contenu du fichier rapport.

Désactivée

Si l'option est activée, la protection e-mail ne génère pas de rapport.
Ne renoncez à la consignation que dans des cas exceptionnels, par ex. uniquement lorsque vous effectuez des tests avec de nombreux virus ou programmes indésirables.

Par défaut

Si l'option est activée, la protection e-mail consigne les informations importantes (sur les résultats positifs, les avertissements et les erreurs) dans le fichier rapport, les informations secondaires sont ignorées pour une meilleure lisibilité. Ce paramètre est activé par défaut.

Étendue

Si l'option est activée, la protection e-mail consigne également les informations secondaires dans le fichier rapport.

Intégrale

Si cette option est activée, la protection e-mail consigne toutes les informations dans le fichier rapport.

Limiter le fichier rapport

Limiter la taille à n Mo

Si l'option est activée, il est possible de limiter la taille du fichier rapport ; valeurs possibles : 1 à 100 Mo. En cas de limitation du fichier rapport, une marge d'environ 50 kilo-octets est laissée pour ne pas trop solliciter l'ordinateur. Si la taille du fichier rapport dépasse la taille indiquée de 50 kilo-octets, les anciennes entrées sont

supprimées automatiquement jusqu'à ce que la taille indiquée moins 50 kilo-octets soit atteinte.

Sauvegarder le fichier rapport avant de le raccourcir

Si l'option est activée, le fichier rapport est sauvegardé avant d'être raccourci.

Écrire la configuration dans le fichier rapport

Si l'option est activée, la configuration utilisée par la protection e-mail est inscrite dans le fichier rapport.

Remarque
Si vous n'avez indiqué aucune limitation du fichier rapport, un nouveau fichier est automatiquement créé lorsque le fichier rapport a atteint une taille de 100 Mo. Une sauvegarde de l'ancien fichier rapport est créée. Jusqu'à trois sauvegardes des anciens fichiers rapport sont conservées. Les sauvegardes les plus anciennes sont supprimées.

12.8 Contrôle parental

Utilisez les fonctions de *CONTRÔLE PARENTAL* d'Avira pour permettre un accès sécurisé à Internet à vos enfants ou autres personnes utilisant votre ordinateur.

- La fonction **Navigation sécurisée** vous permet d'attribuer des rôles aux utilisateurs Windows de votre ordinateur. Vous pouvez définir, pour chaque rôle, des URL ou catégories de contenu autorisées ou interdites, ainsi que la durée d'utilisation quotidienne d'Internet ou les plages horaires autorisées.

Thèmes apparentés :

- En quoi consiste la Navigation sécurisée

12.8.1 Navigation sécurisée

Votre programme Avira possède une fonction **Navigation sécurisée** permettant de filtrer les offres Internet indésirables ou illégales et de limiter la durée d'utilisation d'Internet. La fonction **Navigation sécurisée** fait partie du composant *CONTRÔLE PARENTAL*.

Des rôles peuvent être attribués aux utilisateurs de l'ordinateur. Une rôle peut être configuré et comprend un ensemble de règles avec les critères suivants :

- URL (adresses Internet) interdites ou autorisées
- Catégories de contenu interdits
- Durée d'utilisation d'Internet et plages horaires autorisées pour les jours de la semaine

Des listes de filtres URL performantes sont employées pour le blocage des contenus Internet selon certaines catégories, dans lesquelles les URL sont classifiées dans des

groupes en fonction des contenus des pages Internet. Les listes de filtres URL sont actualisées, adaptées et étendues plusieurs fois par heure. Les rôles **Enfant**, **Adolescent** et **Adulte** sont préconfigurés avec les catégories interdites correspondantes.

Le système détermine la durée d'utilisation d'Internet en fonction des requêtes Internet qui ont lieu à un intervalle minimum de 5 minutes.

Si la fonction **Navigation sécurisée** est active, tous les sites Web appelés dans le navigateur sont contrôlés pendant la navigation Internet, en fonction du rôle. Le site Web est bloqué s'il s'agit d'un site interdit et un message s'affiche dans le navigateur. En cas de dépassement de la durée d'utilisation autorisée, ou en cas d'utilisation en dehors des horaires autorisés, les sites Internet demandés sont bloqués. Un message s'affiche dans le navigateur.

Avertissement
Notez que vous devez activer la fonction **Protection Web** pour pouvoir utiliser la fonction **Navigation sécurisée**.

Avertissement
Protégez la configuration de votre produit Avira par un mot de passe si vous activez la fonction **Navigation sécurisée**. Si la configuration n'est pas protégée par mot de passe, tous les utilisateurs de l'ordinateur peuvent modifier ou désactiver les paramètres de la **Navigation sécurisée**. Vous activez la protection par mot de passe sous Configuration > Généralités > Mot de passe.

Thèmes apparentés :

- Activer la navigation sécurisée
- Attribuer un rôle
- Navigation sécurisée Configuration

Activer la Navigation sécurisée

- Ouvrez l'Avira Control Center et cliquez sur **État** dans la barre de navigation.

  Vous devez activer la fonction **Protection Web** pour pouvoir utiliser la fonction **Navigation sécurisée**.

- Si l'option est inactive, activez la **protection Web** en cliquant sur le bouton rouge à côté de **Protection Web** dans l'affichage **État** sous *Sécurité Internet*.

  Une fois actif, le bouton à côté de la **protection Web** est jaune (« ACTIF »).

  Activez la fonction **Navigation sécurisée** en cliquant sur le bouton rouge à côté de **Navigation sécurisée** dans l'affichage **État**.

  Une fois actif, le bouton à côté de la Navigation sécurisée est vert (« ACTIF »).



- Pour configurer le rôle d'un enfant ou d'une autre personne sous **Navigation sécurisée**, cliquez sur les touches de configuration à côté de **Navigation sécurisée** dans l'affichage **État**.

Thèmes apparentés :

- En quoi consiste la navigation sécurisée
- Attribuer un rôle
- Navigation sécurisée Configuration

Attribuer un rôle

Conditions préalables :

- ✓ Assurez-vous qu'un compte utilisateur Windows a été créé pour chaque personne devant utiliser votre ordinateur. Dans votre produit Avira, vous pouvez attribuer un rôle Navigation sécurisée à chaque compte utilisateur Windows.
- ✓ Activez la fonction **Navigation sécurisée** dans votre produit Avira.
- ✓ Contrôlez les propriétés de chaque rôle avant d'attribuer le rôle à un utilisateur.

- Dans l'affichage **État**, cliquez sur la touche de configuration à côté de **Navigation sécurisée**.
- Sélectionnez l'utilisateur auquel vous souhaitez attribuer un rôle à partir de la liste **Sélection des utilisateurs**.

  La liste contient les comptes utilisateur Windows qui ont été créés sur votre ordinateur.

- Cliquez sur **Ajouter**.

  ↳ L'utilisateur est ajouté à la liste.

  Les rôles utilisateur suivants sont préconfigurés dans Avira Internet Security :

- **Enfant**
- **Adolescent**
- **Adulte**

  Si vous ajoutez un compte utilisateur à la liste, le rôle **Enfant** est attribué par défaut.

- Vous pouvez attribuer un autre rôle en cliquant plusieurs fois sur le rôle d'un utilisateur.

> **Remarque**
> Les utilisateurs de l'ordinateur auxquels n'a été attribué aucun rôle dans la configuration de la fonction **Navigation sécurisée** se voient attribuer par défaut par le programme la qualité d'utilisateur **Standard** avec le rôle **Enfant**. Vous pouvez modifier le rôle de l'utilisateur **standard**.

- Cliquez sur **Appliquer** pour enregistrer la configuration.

Thèmes apparentés :

- Modifier les propriétés d'un rôle
- Ajouter ou supprimer un rôle

Modifier les propriétés d'un rôle

- Dans l'affichage **État**, cliquez sur la touche de configuration à côté de **Navigation sécurisée**.
- Si l'option n'est pas active, cliquez sur le bouton vert à côté du **mode expert**.

  Une fois actif, le bouton à côté du **mode expert** est jaune (« ACTIF »).

  ↳ Les options de **rôles** s'affichent dans la fenêtre de configuration de la fonction **Navigation sécurisée**.
- Cliquez sur le nom du rôle que vous souhaitez modifier (par exemple **Adolescent**), puis sur **Modifier**.

  ↳ La fenêtre avec les **Propriétés** du rôle s'affiche.
- Apportez les modifications puis cliquez sur **OK**.

Thèmes apparentés :

- Propriétés du rôle
- Navigation sécurisée Configuration

Ajouter ou supprimer un rôle

- Dans l'affichage **État**, cliquez sur la touche de configuration à côté de **Navigation sécurisée**.
- Si l'option n'est pas active, cliquez sur le bouton vert à côté du **mode expert**.

  Une fois actif, le bouton à côté du **mode expert** est jaune (« ACTIF »).

  ↳ Les options de **rôles** s'affichent dans la fenêtre de configuration de la fonction **Navigation sécurisée**.
- Pour supprimer un rôle (par exemple **Adolescent**), cliquez sur **Supprimer**.

> **Remarque**
> Vous ne pouvez pas supprimer un rôle tant qu'il est attribué à un utilisateur.

- Pour ajouter un rôle, saisissez un nom de rôle (30 caractères maximum) dans le champ de saisie et cliquez sur **Ajouter**.
- Pour modifier les propriétés du nouveau rôle, sélectionnez le nouveau rôle dans la liste et cliquez sur **Modifier**.

Thèmes apparentés :



- Navigation sécurisée Configuration
- Propriétés du rôle
- Attribuer un rôle

Si vous avez défini un mot de passe pour la fonction **Navigation sécurisée**, la configuration de la **Navigation sécurisée** est masquée et le bouton **Protégé par mot de passe** s'affiche à l'écran.

Protégé par mot de passe

Cliquez sur le bouton « **Protégé par mot de passe** » et définissez un mot de passe pour la « **Navigation sécurisée** » dans la fenêtre « **Saisir mot de passe** » pour activer la configuration de la **Navigation sécurisée**.

Activer la Navigation sécurisée

Si l'option est activée, tous les sites Web appelés lors de la navigation sur Internet sont contrôlés en fonction du rôle attribué dans la **Navigation sécurisée** à l'utilisateur connecté. Les sites Web sont bloqués s'ils ont été classés comme interdits pour le rôle attribué.

> **Remarque**
> Les utilisateurs de l'ordinateur auxquels aucun rôle n'a été attribué dans la configuration de la fonction **Navigation sécurisée** se voient attribuer par le programme la qualité d'utilisateur *Par défaut* avec le rôle **Enfant** si la **Navigation sécurisée** est activée. Vous pouvez modifier le rôle de l'utilisateur par défaut.
> Après l'installation, les rôles d'utilisateur **Enfant**, **Adolescent** et **Adulte** sont créés. La limitation dans le temps de l'utilisation d'Internet est désactivée pour les rôles préconfigurés.

Sélection des utilisateurs

Utilisateur

La liste contient tous les utilisateurs du système.

Ajouter

Ce bouton vous permet d'ajouter l'utilisateur sélectionné à la liste des utilisateurs protégés.

Supprimer

Le bouton supprime une entrée sélectionnée de la liste.



Liste « Utilisateurs - rôle »

La liste affiche tous les utilisateurs ajoutés avec le rôle qui leur a été attribué. Le programme attribue par défaut le rôle **Enfant** lors de l'ajout d'un utilisateur. Un clic de souris sur le rôle affiché vous permet de passer à un autre rôle.

> **Remarque**
> L'utilisateur *par défaut* ne peut pas être effacé.

Rôles (Options disponibles uniquement si le mode expert est activé.)

Champ de saisie

Dans ce champ, saisissez le nom du rôle que vous souhaitez ajouter aux rôles utilisateur.

Modifier

Le bouton **Modifier** vous permet de configurer le rôle sélectionné. Une boîte de dialogue s'affiche à l'écran, dans laquelle vous pouvez définir des URL interdites et autorisées pour le rôle et sélectionner des contenus Internet interdits selon des catégories. (Voir Propriétés du rôle.)

Ajouter

Ce bouton vous permet d'ajouter à la liste des rôles disponibles, le rôle entré dans le champ de saisie.

Supprimer

Le bouton supprime le rôle sélectionné de la liste.

Liste

La liste affiche tous les rôles gérés. Un double-clic sur le rôle affiché vous permet d'ouvrir la boîte de dialogue de définition du rôle.

> **Remarque**
> Les rôles déjà attribués à un utilisateur ne peuvent pas être supprimés.

Thèmes apparentés :

- En quoi consiste la navigation sécurisée
- Propriétés du rôle
- Durée d'utilisation
- Période d'utilisation

Propriétés du rôle

La fenêtre **Propriétés du rôle** vous permet de définir un rôle sélectionné pour l'utilisation d'Internet. (Options disponibles uniquement si le mode expert est activé.)

Vous pouvez autoriser ou interdire explicitement l'accès aux URL. Vous pouvez bloquer certaines catégories de contenus Internet à l'aide de la sélection. Vous avez la possibilité de limiter l'utilisation d'Internet dans le temps.

Contrôler l'accès aux URL suivantes

Cette liste affiche toutes les URL entrées avec les règles *Bloquer* ou *Autoriser*. Le programme attribue par défaut la règle *Bloquer* lors de l'ajout d'une URL. Vous pouvez changer la règle attribuée en cliquant dessus.

Ajouter URL

Saisissez dans ce champ les URL qui doivent être contrôlées par la fonction de contrôle parental. Vous pouvez indiquer des parties de l'URL en signalant le niveau de domaine avec des points finaux ou de début : **nomdedomaine.fr** pour tous les sites et tous les sous-domaines du domaine. Notez un site Web avec un domaine de niveau supérieur quelconque (.com ou .net) avec un point final : nomdedomaine.. Si vous notez une suite de caractères sans point final ou point de début, celle-ci sera interprétée comme un domaine de niveau supérieur, par ex. **net** pour tous les domaines NET (www.domaine.net). Vous pouvez également utiliser le caractère de remplacement ***** pour un nombre quelconque de caractères. Utilisez aussi des points finaux ou de début en combinaison avec les caractères de remplacement, pour repérer les niveaux de domaine.

Remarque
La priorité des règles d'URL est attribuée selon le nombre d'étiquettes de nom (labels) du domaine indiquées. Plus le nombre d'étiquettes de nom du domaine est important, plus la priorité de la règle est élevée. Ex. :
URL : www.avira.com - Règle : autoriser
URL : .avira.com - Règle : bloquer
L'ensemble de règles autorise toutes les URL du domaine www.avira.com. L'URL forum.avira.com est bloquée.

Remarque
Les indications . ou * englobent toutes les URL. Utilisez ces indications quand vous souhaitez par exemple autoriser seulement quelques sites Internet explicitement indiqués pour le rôle *Enfant*, comme par ex. dans l'ensemble de règles suivant :
URL : ***** ou **.** - Règle : bloquer
URL : kids.yahoo.com - Règle : autoriser
URL : kids.nationalgeographic.com - Règle : autoriser



L'ensemble de règles bloque toutes les URL à l'exception des URL avec les domaines kids.yahoo.com et kids.nationalgeographic.com.

Ajouter

Ce bouton vous permet d'ajouter l'URL saisie à la liste des URL contrôlées.

Supprimer

Le bouton supprime l'URL sélectionnée de la liste des URL contrôlées.

Bloque l'accès aux URL faisant partie des catégories suivantes

Si l'option est activée, les contenus Internet figurant parmi les catégories sélectionnées dans la liste sont bloqués.

Durée d'utilisation autorisée

Le bouton **Durée d'utilisation autorisée** vous permet d'ouvrir une boîte de dialogue dans laquelle vous pouvez définir une limitation dans le temps de l'utilisation d'Internet pour le rôle que vous configurez. Vous avez la possibilité de définir l'utilisation d'Internet par mois, par semaine ou avec une différentiation par jours ouvrés et par jours de week-end. Une autre boîte de dialogue permet de définir les périodes d'utilisation précises par jour de la semaine. Voir Durée d'utilisation.

Exemples : URL à contrôler

- `www.avira.com` -OU- `www.avira.com/*`
  = englobe toutes les URL avec le domaine `www.avira.com` :
  www.avira.com/en/pages/index.php, *www.avira.com/en/support/index.html*, *www.avira.com/en/download/index.html*,...
  Les URL avec le domaine www.avira.de ne sont pas incluses.
- `avira.com` -OU- `*.avira.com`
  = comprend toutes les URL avec le domaine de second niveau et de niveau supérieur `avira.com`. L'indication implique tous les sous-domaines existants pour `.avira.com` : *www.avira.com*, *forum.avira.com*,...
- `avira.` -OU- `*.avira.*`
  = comprend toutes les URL avec le domaine de second niveau `avira`. L'indication implique tous les domaines de niveau supérieur ou les sous-domaines existants pour `.avira.` : *www.avira.com, www.avira.fr, forum.avira.com*,...
- `.*domain*.*`
  Comprend toutes les URL contenant un domaine de second niveau avec la chaîne de caractères `domain` : *www.domain.com*, *www.new-domain.fr*, *www.sample-domain1.fr*, ...
- `net` -OU- `*.net`
  = comprend toutes les URL avec le domaine de niveau supérieur `net` :
  www.name1.net, *www.name2.net*,...

Thèmes apparentés :

- En quoi consiste la Navigation sécurisée

- Navigation sécurisée Configuration
- Durée d'utilisation
- Période d'utilisation

Durée d'utilisation

La fenêtre **Durée d'utilisation** vous permet de définir une durée maximum d'utilisation d'Internet pour un rôle utilisateur. Le système détermine la durée d'utilisation d'Internet en fonction des requêtes Internet qui ont lieu à un intervalle minimum de 5 minutes. Le temps de navigation maximum souhaité pour le rôle peut être attribué par semaine, par mois, ou avec une différentiation par jours ouvrés et par jours de week-end.

Limiter l'utilisation d'Internet dans le temps

Cette option vous permet de limiter la durée d'utilisation d'Internet pour tous les utilisateurs de l'ordinateur auxquels le rôle a été attribué. En cas de dépassement de la durée d'utilisation autorisée, les sites Internet demandés par l'utilisateur de l'ordinateur sont bloqués. Un message d'avertissement s'affiche dans le navigateur Web.

Limitation dans le temps par semaine, par mois, par jour (lu-ve, sam-dim)

La durée d'utilisation souhaitée peut être indiquée à l'aide du curseur ou des touches fléchées situées à droite des champs de saisie. Vous pouvez également saisir directement la durée d'utilisation dans les champs horaires. Veuillez tenir compte du format mentionné pour l'indication de temps.

Le programme ne compare pas les différentes durées d'utilisation indiquées. Le programme utilise à chaque fois la valeur pertinente la plus faible pour limiter la durée d'utilisation.

Période d'utilisation précise

Le bouton **Période d'utilisation précise** vous permet d'accéder à une boîte de dialogue dans laquelle vous pouvez définir des horaires par jour pour la durée d'utilisation maximum fixée. Voir Période d'utilisation.

Thèmes apparentés :

- En quoi consiste la Navigation sécurisée
- Navigation sécurisée Configuration
- Propriétés du rôle
- Période d'utilisation

Période d'utilisation

Dans la fenêtre **Période d'utilisation**, vous définissez les horaires d'utilisation autorisés pour la durée d'utilisation d'Internet maximum attribuée pour un rôle : vous pouvez autoriser l'utilisation d'Internet à certains horaires chaque jour de la semaine.

Autoriser l'utilisation d'Internet uniquement dans les périodes indiquées

Cette option vous permet de définir les périodes de navigation pour tous les utilisateurs de l'ordinateur auxquels le rôle configuré a été attribué. Si les utilisateurs de l'ordinateur auxquels un rôle est attribué utilisent Internet en dehors des périodes autorisées, les sites Web demandés sont bloqués. Un message s'affiche dans le navigateur Web.

- Pour autoriser l'utilisation d'Internet à certaines périodes de la journée, sélectionnez les champs horaires souhaités.

  Vous disposez des possibilités suivantes pour sélectionner les périodes de la journée autorisées ou bloquées :

  - **Pour autoriser l'utilisation d'Internet à certaines périodes :** cliquez sur les champs horaires souhaités non sélectionnés ou faites glisser la souris en maintenant le bouton gauche enfoncé sur les champs horaires non sélectionnés.
  - **Pour bloquer l'utilisation d'Internet à certaines périodes :** cliquez sur les champs horaires souhaités sélectionnés ou faites glisser la souris en maintenant le bouton gauche enfoncé sur les champs horaires sélectionnés.

- Avec le bouton droit de la souris, cliquez dans les champs horaires du jour souhaité pour afficher les périodes indiquées dans une boîte de dialogue. Exemple : *utilisation d'Internet bloquée de 00h00 à 11h00.*

Thèmes apparentés :

- En quoi consiste la Navigation sécurisée
- Navigation sécurisée Configuration
- Propriétés du rôle
- Durée d'utilisation

12.9 Protection mobile

Avira ne protège pas uniquement votre ordinateur des virus et logiciels malveillants, mais empêche également la perte et/ou le vol des téléphones portables et smartphones équipés d'un système d'exploitation Android. La liste noire d'Avira Free Android Security vous permet en outre de bloquer les appels et SMS indésirables. Il vous suffit d'ajouter des numéros de téléphone à la liste noire depuis votre journal d'appels, votre journal de SMS ou votre liste de contacts, ou de créer manuellement des contacts que vous souhaitez bloquer.

Vous trouverez de plus amples informations sur notre site Web :

www.avira.com/fr/android

12.9.1 Sécurité pour Android

Avira Free Android Security

Avira Free Android Security comprend deux composants :

- L'application proprement dite, installée sur votre appareil Android
- La console Web Avira Android pour l'enregistrement et le contrôle des fonctionnalités

Configuration requise

Système d'exploitation :

- Android 2.2 (Froyo)
- Android 2.3.x (Gingerbread)
- Android 4.0.x (Ice Cream Sandwich)
- Android 4.1.x (Jelly Bean)

Mémoire vive :

- 1,72 Mo d'espace mémoire interne libre.

Navigateur :

- Mozilla Firefox
- Google Chrome
- Opera
- Internet Explorer 7 ou une version ultérieure.

> **Remarque**
> Notez que Java doit être installé, que JavaScript doit être activé et qu'une connexion Internet opérationnelle est nécessaire.

Caractéristiques de fonctionnement

Si vous ne retrouvez pas votre appareil, Avira Free Android Security vous propose quatre fonctions de protection de vos données personnelles via la console Web Avira Android :

Alerte sonore à distance

Vous déclenchez sur votre appareil une alarme qui retentit pendant 20 secondes.

Suivi de la localisation à distance

Vous activez une commande de localisation qui indique les paramètres de localisation de l'appareil.



Verrouillage à distance

Vous pouvez verrouiller votre appareil instantanément à l'aide d'un code PIN à 4 chiffres.

Suppression à distance

Vous pouvez supprimer des données de la carte SIM ou des cartes mémoire internes et externes. Vous pouvez également restaurer les paramètres d'usine de votre appareil via la console Web.

> **Remarque**
> Pour permettre à une commande de **restauration à distance des paramètres d'usine** de supprimer toutes les données de votre appareil en cas de perte ou de vol, vous devez activer l'option **Administrateur d'appareil** lors de la configuration.

Pour bloquer les appels et SMS indésirables, Avira Free Android Security propose une fonction de liste noire.

Liste noire

Vous pouvez ajouter des contacts à la liste noire depuis le journal d'appels, le journal de SMS ou votre liste de contacts, ou créer manuellement un contact que vous souhaitez bloquer.

Console Web

La console Web Avira est une application qui s'affiche dans un navigateur et qui permet la gestion des fonctions de sécurité. Le tableau de bord de la console Web vous permet de gérer votre compte et de déclencher des fonctionnalités à distance, telles que **Localiser**, **Verrouiller**, **Déclencher une alerte sonore** ou **Supprimer**.

La console Web Avira est composée d'une barre de titre, d'une barre latérale et d'un écran principal avec différents onglets. La barre de titre affiche vos informations de connexion et contient des liens vers la section Support et la gestion de votre compte. Vos appareils enregistrés sont répertoriés dans la barre latérale. L'écran principal de la console Web répertorie toutes les fonctionnalités de sécurité de l'application ainsi que les informations concernant la fonctionnalité **Liste noire** de votre appareil.

La barre de titre de la console Web

Informations sur le compte

La barre de titre contient des liens vous permettant d'accéder au **support technique** d'Avira, à votre **compte**, à vos informations de connexion, et de vous **déconnecter**.





- Cliquez sur le lien **Compte**.
  - ↳ La fenêtre **Informations sur le compte** s'affiche et comporte les champs suivants :

Date de création

Indique la date et l'heure à laquelle vous avez enregistré le compte.

Prénom

Ce champ vous permet d'indiquer votre prénom.

Nom

Ce champ vous permet d'indiquer votre nom de famille.

Langue

Dans le menu déroulant, sélectionnez votre langue préférée.

Pays

Dans le menu déroulant, sélectionnez un pays.

Type de compte

Indique le type de compte que vous utilisez.

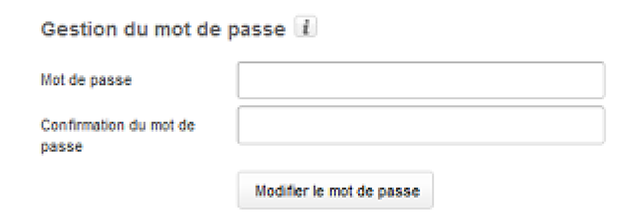
Enregistrer les modifications

- Cliquez sur l'option **Enregistrer les modifications** pour enregistrer les données modifiées sur votre compte.

Gestion des mots de passe

La barre de titre de la console Web Avira contient un lien vers votre **compte** où vous pouvez également gérer votre mot de passe.





- Cliquez sur le lien **Compte**.
  - ↳ La fenêtre **Gestion des mots de passe** s'affiche et comporte les champs suivants :

Mot de passe

Entrez un nouveau mot de passe pour votre compte Avira Free Android Security.

Confirmation du mot de passe

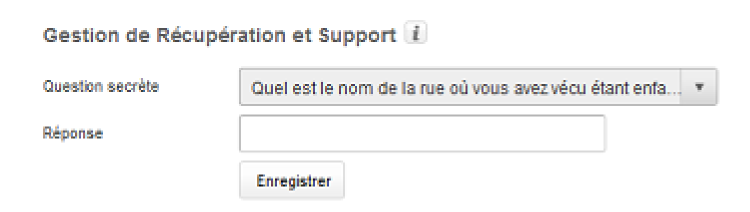
Entrez de nouveau le mot de passe afin de le confirmer.

Modifier le mot de passe

- Cliquez sur ce bouton pour enregistrer les modifications apportées.

Sécurité du compte

La barre de titre de la console Web Avira contient un lien vers votre **compte**, où vous pouvez également définir une question de sécurité. La question de sécurité permet d'améliorer la sécurité de votre compte. Si vous oubliez vos informations de connexion ou si vous souhaitez modifier votre adresse e-mail, vous pouvez vous authentifier à l'aide de la question de sécurité.



- Cliquez sur le lien **Compte**.
  - ↳ La fenêtre **Sécurité du compte** s'affiche et comporte les champs suivants :

Question de sécurité

Ouvre le menu déroulant avec les questions de sécurité ; parmi celles-ci, choisissez-en une à laquelle vous êtes le seul à pouvoir répondre. Cette question doit vous correspondre personnellement.

Réponse

- Entrez votre réponse dans ce champ.



- Assurez-vous que votre réponse ne comporte pas de faute de frappe et que vous vous en souviendrez aisément.

Enregistrer les modifications

- Cliquez sur l'option Enregistrer les modifications pour enregistrer la question de sécurité et votre réponse.

Gestion des appareils

La barre de titre de la console Web Avira contient un lien vers votre **compte**, où vous pouvez également gérer votre appareil.



↳ Cliquez sur le lien **Compte**.

↳ La fenêtre **Gestion des appareils** s'affiche et comporte les champs suivants :

Appareils disponibles

Ouvrez le menu déroulant pour sélectionner un appareil.

Supprimer l'appareil

- Cliquez sur ce bouton pour supprimer l'appareil sélectionné de votre compte.

Comment procéder

Comment modifier mon adresse e-mail ?

Adressez-vous au support d'Avira si vous devez modifier votre adresse e-mail. Votre adresse e-mail ne sert pas uniquement à vous contacter, elle fait aussi office d'identifiant. Par conséquent, vous ne pouvez pas la modifier vous-même à l'aide de la console Web ou via une application de votre appareil.

Comment protéger les données enregistrées sur mon appareil ?

La méthode la plus simple et la plus rapide pour protéger les données enregistrées sur votre appareil consiste à verrouiller celui-ci.

- Connectez-vous à la console Web.
- Accédez à l'onglet **Verrouiller**.
- Entrez un code PIN à 4 chiffres.
- Confirmez le code PIN.



- Cliquez sur **Verrouiller**.
  - ↳ Le code PIN peut désormais être utilisé pour verrouiller et déverrouiller votre appareil.

> **Remarque**
> Le code PIN n'est valable que temporairement. Un nouveau code PIN est nécessaire pour chaque commande de verrouillage/déverrouillage.

Comment déverrouiller mon appareil si j'ai oublié le code PIN ou entré un code PIN incorrect à trois reprises ?

> **Remarque**
> Si vous avez entré un code PIN incorrect à trois reprises sur votre appareil, vous devez le déverrouiller via la console Web. Vous pouvez ensuite envoyer une nouvelle commande de verrouillage à votre appareil.

- Connectez-vous à la console Web.
- Accédez à l'onglet **Verrouiller**.
- Cliquez sur le bouton **Déverrouiller**.
  - ↳ Votre appareil est immédiatement déverrouillé.
- Entrez un nouveau code PIN à 4 chiffres.
- Confirmez le code PIN.
- Cliquez sur **Verrouiller**.
- Cliquez sur **OK** pour confirmer la commande de verrouillage.
  - ↳ Le code PIN peut désormais être utilisé pour verrouiller et déverrouiller votre appareil.

Comment modifier mon code PIN ?

Vous ne pouvez modifier votre code PIN que via la console Web. Il n'est pas possible de le faire via l'application proprement dite.

- Connectez-vous à la console Web.
- Accédez à l'onglet **Verrouiller**.
- Entrez un code PIN à 4 chiffres.
- Confirmez le code PIN.
- Cliquez sur **Verrouiller**.
  - ↳ Le code PIN peut désormais être utilisé pour verrouiller et déverrouiller votre appareil.

Comment retrouver mon appareil en cas de vol ou de perte ?

Si vous avez perdu votre appareil ou s'il vous a été volé, Avira Free Android Security vous propose deux options qui vous permettront de le récupérer :

Déclencher une alerte sonore

La fonctionnalité de déclenchement d'une alerte sonore permet de vous aider à retrouver votre appareil. C'est particulièrement utile si vous l'avez perdu à proximité immédiate, par exemple, dans votre habitation.

- Connectez-vous à la console Web.
- Sélectionnez l'onglet Alerte sonore et cliquez sur Déclencher une alerte sonore.
  - ↳ Votre appareil émet alors un son puissant pendant 20 secondes pour vous aider à le retrouver. L'alerte sonore dure 20 secondes et elle ne peut pas être arrêtée ni interrompue pendant cette période. L'alerte sonore est émise même si votre appareil est en mode silencieux.

> **Remarque**
> L'alerte sonore ne se déclenche pas si l'appareil est éteint ou si la batterie est déchargée.

Localiser l'appareil

Si vous ne savez pas où vous avez perdu votre appareil ou si vous avez des raisons de penser qu'il a été volé, vous pouvez le localiser.

> **Remarque**
> Le processus de localisation peut durer jusqu'à 3 minutes. Vous ne pouvez pas relancer une commande Localiser si le processus est déjà en cours pour un même appareil. Par contre, vous pouvez utiliser la commande Localiser pour un autre appareil enregistré sur votre compte.

- Connectez-vous à la console Web.
- Sélectionnez l'onglet **Localiser**.
  - ↳ Un extrait de Google Maps s'affiche dans la console Web Avira.
- Cliquez sur l'option **Localiser** sous la carte affichée.
- Cliquez sur **OK** pour lancer la localisation.
  - ↳ La durée écoulée du processus de localisation s'affiche. L'emplacement exact de votre appareil sera indiqué sur la carte. Les données géophysiques sont indiquées sous la forme de latitude et de longitude.

Comment enregistrer un nouvel appareil sur un compte existant ?

Vous pouvez ajouter jusqu'à 5 appareils sur votre compte. Tous les appareils, ajoutés au même compte Google ou à la même adresse e-mail via l'application, sont enregistrés sur le même compte Avira Free Android Security. En d'autres termes, un compte de messagerie correspond à un compte Avira Free Android Security pouvant compter jusqu'à 5 appareils différents.

- Utilisez l'appareil que vous souhaitez ajouter à votre compte pour télécharger Avira Free Android Security.
- Installez l'application sur votre appareil.
- Sélectionnez le compte Google ou entrez une autre adresse e-mail et appuyez sur **Accepter le CLUF et continuer**.
  - ↪ Vous recevrez un message à cette adresse, confirmant l'enregistrement d'un nouvel appareil sur votre compte Avira Free Android Security existant.
  - ↪ Si vous vous connectez à la console Web, le nouvel appareil se trouve déjà dans la section **Tous vos appareils**, dans la partie gauche de la console Web.
- Vous pouvez à présent cliquer sur **Modifier** sous l'onglet « Appareil » pour accéder aux paramètres afin de modifier le nom de l'appareil, ainsi que le numéro de téléphone.

> **Remarque**
> Étant donné que vous ne pouvez ajouter que 5 appareils maximum à un compte Avira Free Android Security, vous devez d'abord supprimer un appareil déjà enregistré de votre compte et désinstaller l'application de cet appareil pour pouvoir en enregistrer un nouveau. Accédez d'abord aux paramètres de votre **compte** dans la console Web de votre compte Avira Free Android Security et sélectionnez un appareil dans la liste déroulante de la **gestion des appareils**, puis cliquez sur **Supprimer l'appareil**. Désinstallez ensuite l'application de l'appareil sélectionné.

Résolution de problèmes

Résolution de problèmes

Message



Message	Signification
Connectez-vous à un réseau mobile ou Wi-Fi pour continuer.	Aucune connexion réseau n'a été trouvée pendant le processus d'enregistrement. Activez la connexion au réseau pour continuer.
Le service est actuellement indisponible. Veuillez réessayer plus tard.	Le service Google est actuellement indisponible.
Avira Free Android Security s'est bloqué. Appuyez ici pour nous aider à résoudre le problème.	Une erreur inattendue s'est produite, forçant l'arrêt de l'application. Sélectionnez la notification et confirmez en appuyant sur OK, afin de nous envoyer automatiquement le journal d'erreurs.
Vous avez besoin d'un compte Google pour enregistrer votre appareil. Créez-en un, puis réessayez.	Aucun compte Google n'a été trouvé sur l'appareil.
Le mot de passe de votre compte Google a été modifié. Ouvrez l'application Google Mail ou Google Play pour mettre à jour le mot de passe sur votre appareil.	Le mot de passe du compte Google par défaut sur cet appareil n'est pas valide. Vérifiez si vous avez modifié l'authentification de votre compte Google. Mettez à jour et synchronisez le mot de passe de votre appareil en lançant l'application Google Mail ou Google Play.
Un nombre trop important d'applications sur votre appareil utilisent le service Push de Google (GCM). Désinstallez-en une, puis réessayez.	Google limite le nombre d'applications installées sur votre appareil qui utilisent GCM.

Une erreur s'est produite. Veuillez réessayer plus tard.	Une erreur inconnue s'est produite.
Plus de cinq appareils sont enregistrés avec ce compte. Supprimez-en un pour en ajouter un autre.	Vous avez atteint le nombre maximal de cinq appareils enregistrés sur Avira Free Android Security.
L'appareil n'est plus enregistré sur un compte Avira Free Android Security. L'application a par conséquent été réinitialisée.	Votre enregistrement a été réinitialisé, car cet appareil a été supprimé de la liste des appareils enregistrés.
Une erreur de serveur s'est produite. Veuillez réessayer plus tard.	Une erreur de serveur inconnue s'est produite.
Une erreur inattendue s'est produite, forçant l'arrêt de l'application. Aidez-nous à résoudre ce problème. Cliquez sur OK, et nous recevrons automatiquement le journal d'erreurs. Vous pouvez également ajouter des commentaires concernant ce problème :	Une erreur inattendue a fermé l'application.
Erreur inattendue. Consultez la barre de notification pour plus d'informations.	Une erreur inattendue s'est produite.
Merci beaucoup !	Merci d'avoir signalé le problème, les informations ont été correctement envoyées.
En cas de perte ou de vol de votre appareil, Avira Free Android Security vous permet de restaurer les paramètres d'usine pour effacer les données de l'appareil. Afin d'effectuer cette opération, la fonction Administrateur d'appareil doit être activée.	Si vous avez perdu votre appareil, Avira Free Android Security vous permet d'effacer les données qu'il contient à l'aide d'une restauration des paramètres d'usine. Pour ce faire, la fonction **Administrateur d'appareil** doit être activée.

Effacement via restauration des paramètres d'usine activé/désactivé.	La fonction d'effacement avec la commande de **restauration des paramètres d'usine** est activée/désactivée.
Votre appareil a bien été enregistré auprès d'Avira Free Android Security.	Avira Free Android Security a bien été enregistré.
Un e-mail a été envoyé à <jean.dupont@gmail.com>. Consultez votre compte de messagerie pour obtenir plus d'informations, ainsi que d'autres instructions.	Un e-mail contenant des informations d'activation a été envoyé à <jean.dupont@gmail.com>. Consultez ce message pour commencer à utiliser notre logiciel.
En cas de questions, consultez le forum de support ou contactez un collaborateur d'Avira.	En cas de questions, consultez notre forum ou contactez l'un de nos collaborateurs.
L'enregistrement a échoué. Redémarrez l'application, puis réessayez.	Une erreur inattendue s'est produite au cours du processus d'enregistrement. Redémarrez l'application et essayez à nouveau de vous enregistrer.
L'enregistrement a échoué. Il se peut que vous utilisiez une technologie incompatible avec Avira Free Android Security. Redémarrez l'application, puis réessayez.	Il se peut que votre appareil utilise une technologie incompatible avec Avira Free Android Security. Respectez la configuration requise suivante : Système d'exploitation : Android 2.2 (Froyo) - Android 4.1. (Jelly Bean). Mémoire vive : 1,28 Mo d'espace mémoire libre. Navigateurs : Mozilla Firefox, Google Chrome, Opera et Internet Explorer 7 ou une version ultérieure.
Erreur de création du contact	Impossible d'ajouter le contact à la liste noire car il s'y trouve déjà.
Nom déjà dans la liste noire	Ce nom se trouve déjà dans la liste noire, il ne peut donc pas être ajouté une deuxième fois.

Contact déjà dans la liste noire	Ce contact se trouve déjà dans la liste noire, il ne peut donc pas être ajouté une deuxième fois.
Numéro déjà dans la liste noire pour <Jean Dupont>	Ce numéro de téléphone se trouve déjà dans la liste noire et est associé au contact <Jean Dupont>, il ne peut donc pas être ajouté une deuxième fois.

Glossaire

Abréviation/terme	Signification
GCM	Le service Android Google Cloud Messaging (GCM) de Google permet d'envoyer des données depuis des serveurs vers les applications installées sur votre appareil.
IMEI	L'International Mobile Equipment Identity (littéralement : identité internationale d'équipement mobile) est un numéro unique, semblable à une empreinte digitale, permettant d'identifier les appareils.
Carte SIM	La carte SIM (Subscriber Identification Module, soit : module d'identification de l'abonné) est une carte de fournisseur, sur laquelle différentes informations sont enregistrées, telles que le numéro de série, le numéro de téléphone et votre code PIN.
PIN	Le code PIN (Personal Identification Number) est le numéro d'identification personnel, généralement constitué d'un nombre à 4 chiffres.

SE	Système d'exploitation de votre appareil.
GPS	Le Global Positioning System (littéralement : système de localisation mondial) est un système par satellites qui fournit des données temporelles et de localisation à des récepteurs GPS.
Tour de transmission cellulaire	Technologie radio avancée qui capte les signaux des téléphones mobiles et les transmet à d'autres tours, à l'aide d'ondes radio.
Wi-Fi	Il s'agit d'une norme qui permet l'échange de données et l'accès sans fil à Internet.
WLAN	Accès au réseau sans fil.
Cloud	Il s'agit d'une infrastructure informatique et d'un emplacement de serveur distant. Les données enregistrées dans le cloud ne sont pas enregistrées localement sur l'ordinateur.
Autre numéro de téléphone	Numéro de téléphone auquel vous pouvez être contacté à l'aide du bouton **Appeler le propriétaire** sur l'appareil verrouillé.
Latitude	Coordonnée géographique qui indique la position nord-sud sur Terre.
Longitude	Coordonnée géographique qui indique la position est-ouest sur Terre.

Service

Support

Service de support

Vous trouverez toutes les informations nécessaires concernant notre service complet de support sur notre page Web http://www.avira.com.

Forum de la communauté

Avant de contacter notre service d'assistance téléphonique, nous vous recommandons de consulter notre forum d'utilisateurs à l'adresse http://forum.avira.com.
Il se peut que votre problème ait déjà été évoqué et résolu au sein de la communauté.

FAQ

Passez également en revue la section FAQ, disponible sur notre site Web :
http://www.avira.com/fr/support-for-home-knowledgebase
. Il se peut que votre question y ait déjà été posée et qu'une réponse ait déjà été publiée par d'autres utilisateurs.

Contact

Adresse

Avira Operations GmbH & Co. KG
Kaplaneiweg 1
D-88069 Tettnang
Allemagne

Internet

Vous trouverez davantage d'informations nous concernant et relatives à nos produits à l'adresse suivante :
http://www.avira.com

Utilisation

Console Web

Une fois l'installation terminée, vous devez enregistrer votre appareil pour accéder à la console Web Avira.

- La console Web Avira est composée d'une barre de titre, d'une barre latérale et d'un écran principal avec différents onglets.
- La barre de titre affiche vos informations de connexion et contient des liens vers la section Support et la gestion de votre compte. En outre, vous pouvez sélectionner les paramètres linguistiques de la console Web Avira à cet endroit.
- Vos appareils enregistrés sont répertoriés dans la barre latérale.
- Chaque appareil s'affiche dans un champ distinct :
  - Cliquez sur le bouton **Modifier** présent dans le champ relatif à l'appareil pour accéder à l'onglet **Paramètres** de la console Web, depuis lequel vous pouvez gérer le nom et le numéro de téléphone de votre appareil.
- Dans le bas de la barre latérale, un lien vous permet d'indiquer et d'enregistrer une question de sécurité personnelle.

- L'écran principal de la console Web répertorie toutes les fonctionnalités de sécurité permettant de contrôler votre appareil Android ainsi que les informations concernant le contenu de votre liste noire.

Onglets de la console Web

La console Web comporte les onglets suivants :

- Tableau de bord
- Localiser
- Effacer
- Alerte sonore
- Verrouiller
- Liste noire
- Paramètres

Tableau de bord de la console Web Avira Free Android Security

L'onglet **Tableau de bord** contient différentes informations sur chaque appareil ainsi que des boutons de commande permettant de déclencher des actions visant à protéger l'appareil.



Informations sur l'appareil

- Marque : marque de l'appareil.
- Modèle : désignation du modèle de l'appareil.
- IMEI : l'International Mobile Equipment Identity (littéralement : identité internationale d'équipement mobile) est un numéro unique à 15 chiffres, permettant d'identifier les téléphones mobiles et certains téléphones satellite.
- Version du SE : numéro de version du système d'exploitation Android.
- Version de l'application : numéro de version de l'application Avira installée. Si vous utilisez une version obsolète, un symbole d'avertissement s'affiche en rouge.
- Gest. appareils : indique si la gestion des appareils est active. Si elle est désactivée, un symbole d'avertissement s'affiche en rouge.
- Batterie : informations concernant le niveau de charge de la batterie (en pourcent).
- Numéro de téléphone : numéro de téléphone enregistré sur la carte SIM.
- Réseau : réseau mobile auquel la carte SIM appartient.
- Pays : pays d'origine de la carte SIM.
- **Actualiser** : bouton d'actualisation permettant de mettre à jour les informations sur l'appareil.

Suivi de la localisation



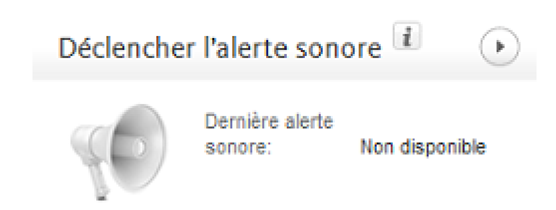
- Dernière localisation : moment de la dernière localisation de l'appareil, par ex. « il y a 5 heures », « il y a 3 jours ».
- Latitude : latitude exacte de l'emplacement de l'appareil.
- Longitude : longitude exacte de l'emplacement de l'appareil.

Verrouiller l'appareil



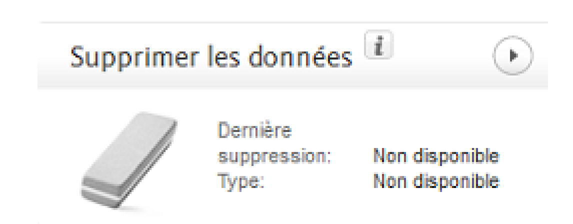
- Dernière action : dernière action effectuée via la console Web, par ex. « Verrouiller ».
- Dernier déclenchement : moment du dernier verrouillage / déverrouillage de l'appareil.

Déclencher une alerte sonore



- Dernier déclenchement : période écoulée depuis le dernier envoi d'une alerte à l'appareil.

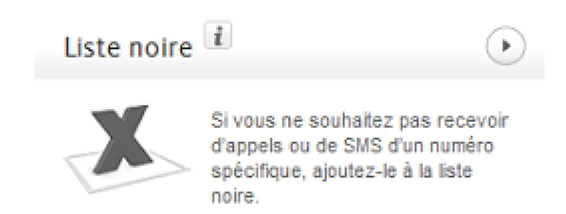
Supprimer les données



- Dernier effacement : période écoulée depuis le dernier effacement sur l'appareil.
- Type : type d'action d'effacement effectuée sur l'appareil.



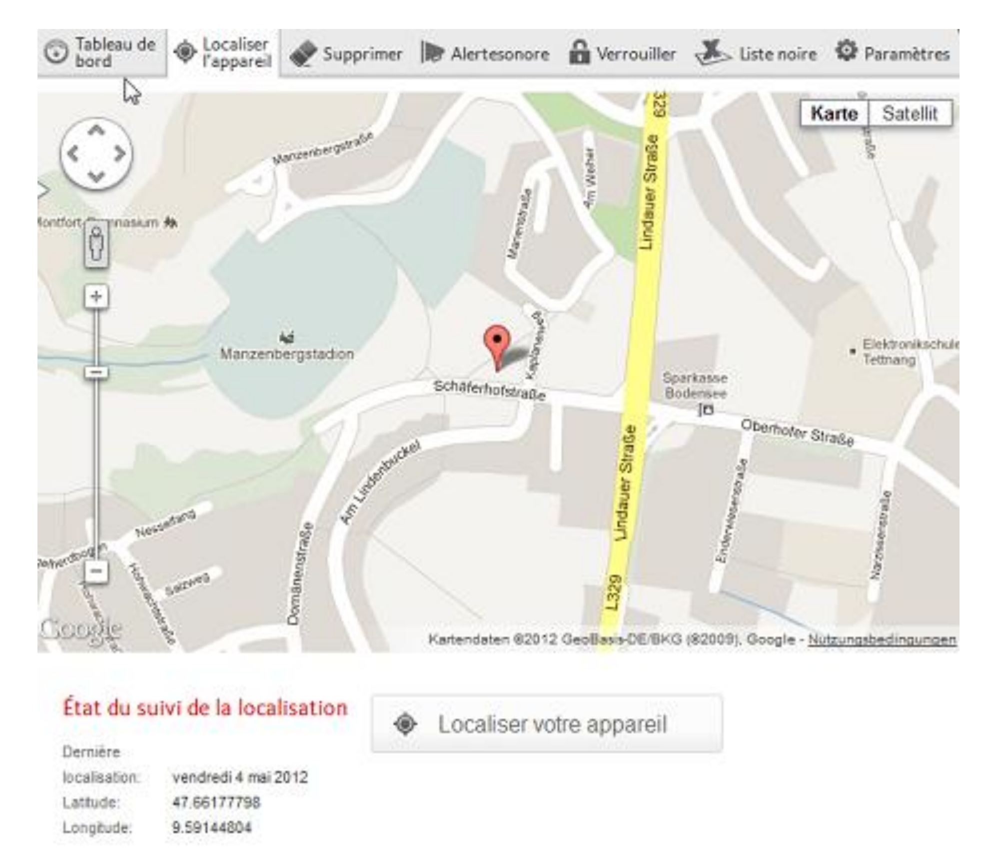
Liste noire



- Cette fonction permet de bloquer des appels et SMS indésirables.

Localiser

L'onglet **Localiser** affiche un extrait de Google Maps. Le statut du suivi de la localisation est affiché sous la carte.



- Cliquez sur le bouton **Localiser** pour lancer la localisation de l'appareil égaré.
  - ↳ La localisation peut prendre quelques minutes, en fonction des performances du réseau et de la force du signal.

  Avira Free Android Security recherche l'appareil via GPS, tours de transmission cellulaire et réseau local sans fil.

  La durée écoulée du processus de localisation s'affiche.
  - ↳ L'emplacement exact de l'appareil égaré est ensuite indiqué sur la carte. Vous pouvez effectuer un zoom avant ou arrière sur la carte.



Effacer

> **Remarque**
> Si votre version d'Avira Free Android Security ne prend pas en charge la fonction d'**effacement**, mettez l'application à jour sur votre appareil en suivant les instructions décrites dans notre base de connaissances. Ensuite, il vous suffit d'actualiser cette page pour accéder à l'ensemble des fonctionnalités de la **fonction d'effacement**.

Trois options de suppression de données sont disponibles sous l'onglet Effacer. Vous pouvez également sélectionner une combinaison de ces options d'effacement. La fonction d'effacement entraîne la suppression définitive des données. En d'autres termes, les données supprimées par cette procédure ne peuvent pas être restaurées.

> **Remarque**
> Il est fortement recommandé de verrouiller votre appareil avant de déclencher une commande d'effacement. Pensez à sauvegarder régulièrement vos données importantes. Car, si les circonstances vous contraignent à recourir à une suppression à distance des données de votre appareil, vous n'avez plus la possibilité d'effectuer une sauvegarde.

Carte SIM

La fonction d'effacement de la **carte SIM** supprime toutes les données de votre carte SIM. Toutes les informations de contact et les SMS enregistrés sur la carte SIM sont supprimés. Une fois supprimées, ces données ne peuvent plus être restaurées. L'effacement de la carte SIM n'affecte pas les données enregistrées sur votre appareil ou sur la carte SD.



Carte SIM

> **Remarque**
> Selon le type de carte, l'effacement de la **carte SIM** n'est pas toujours possible.

- Cliquez sur **Carte SIM** pour supprimer toutes les données enregistrées sur la carte SIM.
- Confirmez la suppression en cliquant sur **OK**.
  - ↳ Le message **La carte SIM a été effacée !** s'affiche.
- Cliquez sur **OK** pour fermer le message et revenir sous l'onglet **Effacer**.

Toute la mémoire

La fonction d'effacement de **toute la mémoire** supprime toutes les données enregistrées sur votre appareil ou votre carte SD. Une fois supprimées, ces données ne peuvent plus être restaurées. L'effacement de **toute la mémoire** n'affecte pas les données enregistrées sur la carte SIM.



- Cliquez sur **Effacer la mémoire** pour supprimer les données enregistrées directement sur votre appareil ou sur la carte SD.
- Confirmez la suppression en cliquant sur **OK**.
  - ↳ Le message **La mémoire a été effacée !** s'affiche.
- Cliquez sur **OK** pour fermer le message et revenir sous l'onglet **Effacer**.

Restauration des paramètres d'usine

L'option **Restauration des paramètres d'usine** rétablit les paramètres par défaut de votre appareil et supprime également tous les comptes, applications et données d'application de l'appareil. La **restauration des paramètres d'usine** n'affecte pas les données enregistrées sur la carte SIM ou sur la carte SD.



Remarque
Pour permettre à une commande de **restauration à distance des paramètres d'usine** de supprimer toutes les données de votre appareil en cas de perte ou de vol, vous devez activer la fonction **Administrateur d'appareil** lors de la configuration.

- Cliquez sur **Restauration des paramètres d'usine** pour rétablir les paramètres par défaut de votre appareil.
- Confirmez ce type de suppression en cliquant sur **OK**.
- Cliquez à nouveau sur **OK** pour continuer.
- Pour fermer le message vous informant de la réussite de la **restauration des paramètres d'usine**, cliquez sur **OK**.

Avertissement
La **restauration des paramètres d'usine** désinstalle également Avira Free Android Security. Vous ne serez alors plus en mesure de transmettre des commandes à votre appareil via la console Web, par ex. vous ne pourrez plus verrouiller ni localiser votre appareil.



Suppression groupée

L'option de **suppression groupée** vous permet de recourir à un, deux ou trois types d'effacement à la fois.

- Sélectionnez les types d'effacement que vous souhaitez utiliser ou cliquez sur **Tout sélectionner** pour lancer tous les types d'effacement en une fois.
- Cliquez sur **Lancer les actions d'effacement sélectionnées**.
- Confirmez votre choix en cliquant sur **OK**.
  - ↳ Selon votre sélection et la taille de la mémoire de votre appareil, cette action peut prendre jusqu'à 60 minutes.
- Cliquez sur **OK** pour continuer.
- Pour fermer le message vous informant de la réussite de la **suppression groupée**, cliquez sur **OK**.

Les effets des trois **actions d'effacement** sont les suivants :

Mémoire affectée	Carte SIM	Toute la mémoire	Restauration des paramètres d'usine
SMS sur l'appareil			suppression
SMS sur la carte SIM	suppression		
Contacts sur l'appareil			suppression
Contacts sur la carte SIM	suppression		
Données de la carte SD		suppression	
Données de la mémoire USB interne		suppression	



Comptes, applications, données d'application			suppression

Alerte sonore

L'onglet **Alerte sonore** vous permet de déclencher un son puissant émis par votre appareil. Cette fonction vous aide à retrouver rapidement votre appareil.



- Cliquez sur le bouton **Déclencher une alerte sonore** pour lancer cette fonction.
- Cliquez sur **OK** pour confirmer l'alerte sonore.
  - ↳ Votre appareil émet un son puissant pendant 20 secondes. L'alerte sonore ne peut pas être arrêtée ni interrompue pendant ce laps de temps.

Verrouiller

Pour verrouiller ou déverrouiller votre appareil, vous pouvez entrer un code PIN à 4 chiffres sous l'onglet **Verrouiller**. Vous pouvez entrer un message personnalisé qui s'affichera sur l'écran de verrouillage de votre appareil. Vous pouvez ajouter un numéro de téléphone à appeler à l'aide du bouton **Appeler le propriétaire** sur l'appareil verrouillé.



Remarque
Il est fortement recommandé de verrouiller votre appareil avant de déclencher une commande d'effacement. Pensez à sauvegarder régulièrement vos données importantes. Car, si les circonstances vous contraignent à recourir à

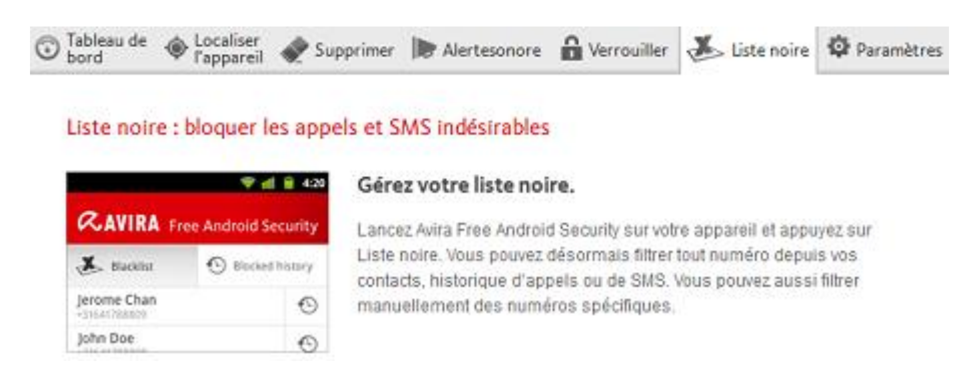


une suppression à distance des données de votre appareil, vous n'avez plus la possibilité d'effectuer une sauvegarde.

- Entrez un code PIN à 4 chiffres dans le champ **Entrer code PIN**.
- Confirmez votre code PIN dans le champ situé en dessous.
- Cliquez sur **OK** pour déclencher le verrouillage.
  - ↳ Pour le déverrouiller, entrez le code PIN à 4 chiffres sur votre appareil ou cliquez sur l'onglet **Verrouiller** dans votre compte de la console Web et sélectionnez le bouton **Déverrouiller**.
  - ↳ Si vous avez défini un code PIN précédemment, vous ne pouvez déverrouiller votre appareil que manuellement. Si vous avez oublié votre code PIN, vous devez déverrouiller votre appareil via le bouton **Déverrouiller** de votre compte de la console Web.
- Dans le champ **Message en cas de perte**, entrez un message à afficher sur votre appareil verrouillé. Rédigez par exemple un texte suivi de votre adresse e-mail afin que la personne qui le trouve puisse vous contacter facilement.
- Dans le champ **Autre numéro de téléphone**, entrez un numéro de téléphone grâce auquel vous pouvez être contacté à l'aide du bouton **Appeler le propriétaire** sur l'appareil verrouillé. Utilisez un numéro fiable, tel que votre numéro de téléphone fixe ou le numéro d'un ami.
- Cliquez sur **Verrouiller** pour enregistrer le code PIN sur votre appareil.
- Cliquez sur **OK** pour verrouiller votre appareil.
- Cliquez sur **Déverrouiller** si vous souhaitez déverrouiller votre appareil à l'aide de la console Web.

Liste noire

Si vous ne voulez pas être dérangé par certains appels et SMS, vous pouvez simplement ajouter ces numéros à la liste noire. Cette fonction vous permet de bloquer des appels et SMS indésirables. Vous pouvez ajouter des numéros à partir de vos contacts, de votre journal d'appels et de vos messages, ou entrer manuellement un numéro.



Ajouter des numéros à la liste noire depuis les journaux de votre appareil

Ajoutez simplement des numéros à la liste noire depuis vos journaux d'appels et de messages ou depuis vos contacts.

- Ouvrez Avira Free Android Security sur votre appareil.
- Sélectionnez **Liste noire**.
  - ↳ L'écran **Liste noire** s'affiche.
- Sélectionnez le bouton **Ajouter**.
  - ↳ L'écran **Ajouter les contacts à la liste noire** s'affiche.
- Sélectionnez le champ correspondant au journal depuis lequel vous souhaitez ajouter un numéro à la liste noire.

  Si vous ne souhaitez pas ajouter de numéro à la liste noire, appuyez sur **Annuler**.

  Sélectionnez le numéro que vous souhaitez bloquer.
  - ↳ L'écran **Entrer les coordonnées** affiche le numéro et le nom du contact que vous souhaitez bloquer.
- Sélectionnez une option de liste noire. Vous disposez des options **Appels et SMS**, uniquement **Appels** ou uniquement **SMS**.
- Cliquez sur **Enregistrer** afin d'enregistrer le numéro dans la liste noire.
- Le numéro bloqué s'affiche sur l'écran **Liste noire**.

> **Remarque**
> Si le contact que vous souhaitez ajouter se trouve déjà dans la liste noire, vous recevez un message d'erreur.

Ajouter manuellement des numéros à la liste noire

Vous pouvez également entrer manuellement des numéros dans la liste noire.

- Ouvrez Avira Free Android Security sur votre appareil.
- Sélectionnez **Liste noire**.
  - ↳ L'écran **Liste noire** s'affiche.
- Sélectionnez le bouton **Ajouter**.
  - ↳ L'écran **Ajouter les contacts à la liste noire** s'affiche.
- Sélectionnez l'option **Créer un contact manuellement** si vous souhaitez entrer un numéro.
  - ↳ L'écran **Entrer les coordonnées** s'affiche.
- Touchez le champ **Nom** afin d'accéder au clavier permettant d'entrer les lettres.
- Touchez le champ **Numéro de téléphone** afin d'accéder au clavier permettant d'entrer les chiffres.

- Sélectionnez une option de liste noire. Vous disposez des options **Appels et SMS**, uniquement **Appels** ou uniquement **SMS**.
- Cliquez sur **Enregistrer** afin d'enregistrer le numéro dans la liste noire.
- Le numéro bloqué s'affiche sur l'écran **Liste noire**.

Modifier la liste noire

Vous pouvez modifier le numéro de téléphone et le nom de votre contact bloqué.

- Ouvrez Avira Free Android Security sur votre appareil.
- Sélectionnez **Liste noire**.
  - ↳ L'écran **Liste noire** s'affiche.
- Sélectionnez le contact que vous souhaitez modifier.
  - ↳ L'écran **Modifier le contact bloqué** s'affiche.
- Touchez le champ **Nom** afin d'accéder au clavier permettant de modifier le nom.
- Touchez le champ **Numéro de téléphone** afin d'accéder au clavier permettant de modifier le numéro.
- Cliquez sur **Enregistrer** afin d'enregistrer le contact modifié dans la liste noire.
- Cliquez sur **Annuler** si vous ne souhaitez pas enregistrer les modifications effectuées.

Événements bloqués

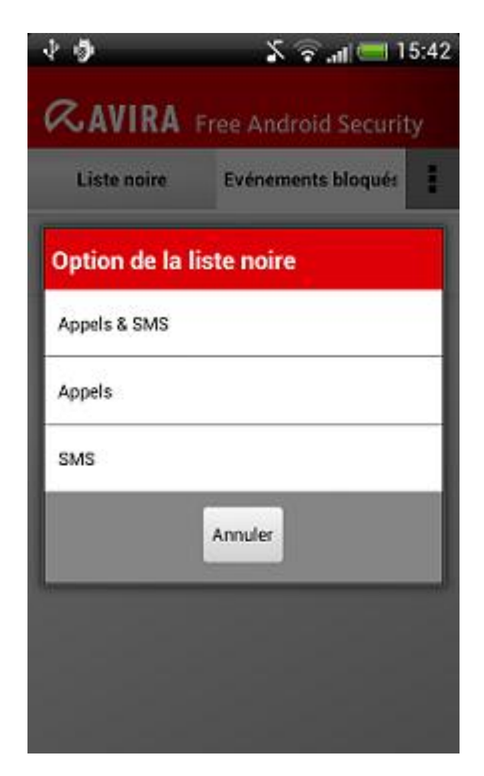
Vous pouvez consulter l'historique de tous vos contacts bloqués sous l'onglet **Événements bloqués**. Vous pouvez filtrer la liste à l'aide de certaines options. Le nom du contact, la date, l'heure, ainsi que le type de tentative de contact sont affichés.

- Sélectionnez le bouton **Tous** pour pouvoir sélectionner les événements suivants : **Tous**, **Aujourd'hui** ou **Nouveau**.
- Sélectionnez le bouton **Appels et SMS** pour afficher à la fois les appels et messages bloqués. Sélectionnez l'option **Appels** pour vérifier quels sont les contacts bloqués qui ont tenté de vous appeler. Sélectionnez l'option **SMS** pour afficher les messages provenant des numéros bloqués.

Supprimer des entrées des événements bloqués

Vous pouvez supprimer des entrées des **événements bloqués**. Filtrez la liste des événements bloqués en fonction des paramètres suivants : **Tous**, **Aujourd'hui** ou **Nouveau,** et sélectionnez l'option **Appels et SMS**, **Appels** ou **SMS**. Vous pouvez supprimer tous les événements ou le faire individuellement. Par exemple, si vous filtrez sur **Tous** et **Appels**, tous les appels bloqués sont répertoriés. Vous avez alors la possibilité de supprimer chronologiquement tous les appels bloqués de vos contacts. Ou vous sélectionnez certains contacts et ne supprimez que les appels affichés.





- Sélectionnez le contact dont vous souhaitez supprimer les événements bloqués.
  - ↳ L'heure et le nombre d'appels et/ou SMS reçus s'affichent.
- Sélectionnez le champ **SMS** pour afficher le contenu des SMS bloqués.
  - ↳ Vous pouvez alors ouvrir et lire les messages.
  - ↳ Vous pouvez supprimer tous les SMS ou le faire individuellement.

  L'option **Sélectionner tout** permet de sélectionner tous les SMS pour suppression ; vous pouvez également sélectionner les SMS individuellement.

  Sélectionnez l'option **Supprimer** pour supprimer tous ces messages, ou appuyez sur **Retour** pour annuler la suppression.

  - ↳ Vous êtes invité à confirmer la suppression des SMS bloqués.

  Appuyez sur **Supprimer** pour supprimer les SMS sélectionnés de l'historique.

  Appuyez sur **Annuler** pour arrêter la suppression.
- Sélectionnez le champ **Appels** pour afficher tous les appels de vos contacts bloqués.
  - ↳ Vous pouvez supprimer tous les appels ou le faire individuellement.

  L'option **Sélectionner tout** permet de sélectionner tout l'historique des appels pour suppression ; vous pouvez également sélectionner les appels individuellement.

  Sélectionnez l'option **Supprimer** pour supprimer tous ces appels, ou appuyez sur **Retour** pour annuler la suppression.

  - ↳ Vous êtes invité à confirmer la suppression des appels bloqués.

  Appuyez sur **Supprimer** pour supprimer les appels sélectionnés de l'historique.

Appuyez sur **Annuler** pour arrêter la suppression.

Rapports

L'onglet **Paramètres** comporte la section **Rapport d'activités** qui permet d'afficher toutes les activités d'Avira Free Android Security effectuées à l'aide de la console Web.

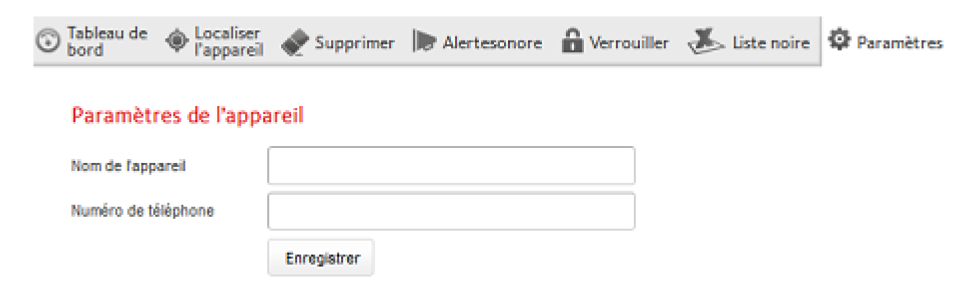
Les informations répertoriées sont classées par date et heure.

Exemple d'informations affichées par le rapport d'activités :

Date	Heure	Message
Mardi 7 août 2012	15:17	Informations sur l'appareil actualisées
Mardi 7 août 2012	14:05	Appareil localisé
Lundi 13 août 2012	18:11	Appareil déverrouillé

Paramètres

L'onglet Paramètres vous permet de gérer le nom et le numéro de téléphone de votre appareil. En outre, la section **Rapports** permet de vérifier toutes les activités d'Avira Free Android Security effectuées à l'aide de la console Web.



- Dans la barre de navigation, cliquez sur l'appareil que vous souhaitez gérer.
- Entrez le nom de votre appareil dans le champ **Nom de l'appareil**.
- Entrez le numéro de téléphone de cet appareil dans le champ **Numéro de téléphone**.
- Cliquez sur **Enregistrer les modifications** pour enregistrer les paramètres que vous avez définis pour cet appareil.



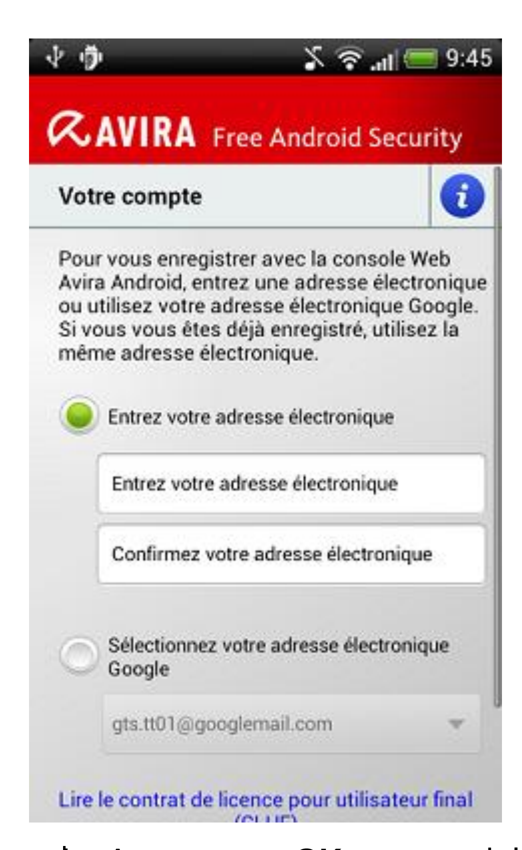
↳ La console Web Avira Android indique que les paramètres ont bien été enregistrés.

Installation et désinstallation

Installation et désinstallation d'Avira Free Android Security

Téléchargement et installation

Téléchargez l'application Avira Free Android Security directement depuis Google Play sur votre appareil et installez-la. Une fois l'installation terminée, les nouvelles fonctions vous sont présentées. Ensuite, vous êtes invité à enregistrer votre appareil via l'écran d'enregistrement d'Avira Free Android Security. Pour ce faire, vous pouvez utiliser votre compte Google ou une adresse e-mail créée auprès d'un autre fournisseur. Une connexion Internet stable est nécessaire pour effectuer cette procédure.



- Appuyez sur **OK** pour ouvrir le formulaire d'enregistrement.
- Entrez votre compte Google ou une autre adresse e-mail.
- Appuyez sur **Accepter le CLUF et continuer** pour poursuivre.

  ↳ Vous recevrez un message de confirmation d'Avira pour votre nouveau compte Avira Free Android Security à l'adresse e-mail indiquée. Ce message de confirmation comprend un lien vous permettant de définir un mot de passe personnel pour vous connecter à la console Web Android.



- Cliquez sur le lien repris dans le message de confirmation pour définir un mot de passe et activer la console Web Android.
  - ↳ La console Web vous permet désormais de contrôler à distance vos appareils.

Pour permettre à Avira Free Android Security de supprimer toutes les données à l'aide de la commande **Restauration des paramètres d'usine**, par exemple, en cas de perte ou de vol de l'appareil, vous devez activer la fonction **Administrateur d'appareil** lors de la configuration :

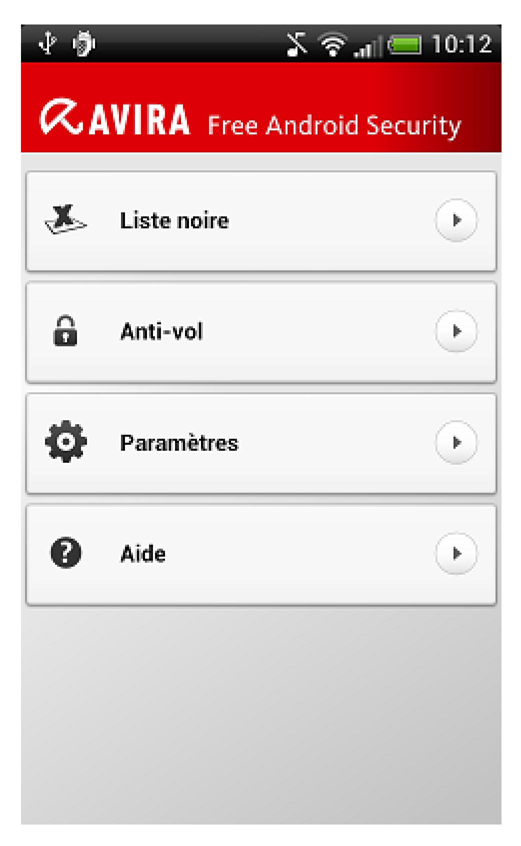


- Appuyez sur le bouton **Activer** pour activer la fonction **Administrateur d'appareil**.
  - ↳ La boîte de dialogue **Activer l'administrateur d'appareil** s'affiche.
- Confirmez l'activation de l'**administrateur d'appareil** en appuyant sur le bouton **Activer**.
  - ↳ De cette manière, vous autorisez Avira Free Android Security à effacer toutes les données de votre appareil au cas où vous souhaiteriez exécuter la commande de **restauration des paramètres d'usine**.

Si vous hésitez à installer l'**administrateur d'appareil** pendant la configuration, vous pouvez activer cette option de configuration ultérieurement. Procédez comme suit :

- Ouvrez Avira Free Android Security sur votre appareil.





- Appuyez sur le bouton **Paramètres**.
  - ↳ Vous pouvez vérifier si l'option d'**effacement grâce à une commande de restauration des paramètres d'usine** est activée.
- Appuyez sur le champ **Paramètres d'effacement**.
  - ↳ La boîte de dialogue **Activer l'administrateur d'appareil** s'affiche. Vous êtes invité à activer la fonction **Administrateur d'appareil**.
- Appuyez sur le bouton **Activer** situé dans le bas de la boîte de dialogue.
- Confirmez l'activation de l'**administrateur d'appareil** en appuyant sur le bouton **Activer**.
  - ↳ Vous pouvez alors voir que la fonction d'**effacement grâce à une commande de restauration des paramètres d'usine** est activée.

> **Remarque**
> Vous pouvez activer et désactiver l'**administrateur d'appareil** à tout moment sur votre appareil via l'application Avira Free Android Security. Sélectionnez **Paramètres > Paramètres d'effacement > Effacement via restauration des paramètres d'usine > Activer / Désactiver**.

Installation via un ordinateur

Vous pouvez télécharger l'application Avira Free Android Security via votre ordinateur.

- Ouvrez Google Play sur votre ordinateur.

- Recherchez l'application Avira Free Android Security.
- Cliquez sur **Installer** pour télécharger l'application sur votre ordinateur.
  - ↳ Vous êtes invité à vous connecter pour installer l'application.
- Cliquez sur **Se connecter** pour accéder à votre compte Google.
- Entrez vos informations de connexion.
- Cliquez sur **OK** pour télécharger l'application vers un appareil sélectionné.
  - ↳ L'application Avira Free Android Security est téléchargée sur cet appareil.
- Cliquez sur **OK** pour fermer la boîte de dialogue de téléchargement.
  - ↳ Le site Web de Google Play s'affiche à nouveau et le bouton **Installé** indique que l'application est déjà téléchargée sur l'appareil.

Désinstallation

Pour désinstaller Avira Free Android Security, deux étapes sont nécessaires. Vous devez désinstaller l'application de votre appareil et supprimer l'appareil de votre compte Avira Free Android Security.

> **Remarque**
> Assurez-vous que la fonction **Administrateur d'appareil** est désactivé sur votre appareil avant de désinstaller Avira Free Android Security.

Si vous souhaitez désinstaller Avira Free Android Security, vous pouvez utiliser l'assistant de désinstallation de l'application ou le gestionnaire d'applications de votre appareil.

Si vous utilisez l'assistant de désinstallation de l'application, passez du bouton **Aide** au bouton **Procéder à la désinstallation**.

- Appuyez sur **Aide > Procéder à la désinstallation > Vers la désinstallation**.
  - ↳ Les informations d'état de votre administrateur d'appareil s'affichent.
- Si nécessaire, appuyez sur **Administrateur d'appareil** pour désactiver cette fonction.
- Appuyez sur **Suivant** pour poursuivre le processus de désinstallation.
  - ↳ L'écran de sondage relatif à la désinstallation s'affiche.
- Sélectionnez toutes les réponses qui s'appliquent à votre situation.
- Vous pouvez nous faire part de vos remarques détaillées dans le champ de commentaire.
- Appuyez sur **Suivant** pour poursuivre la désinstallation.
- Appuyez sur **OK** pour terminer le processus de désinstallation.



Si vous voulez désinstaller l'application via le gestionnaire d'applications de votre appareil, accédez à la fonction de **gestion des applications** depuis le bouton **Paramètres**.

- Sélectionnez l'application Avira Free Android Security et sélectionnez l'option **Désinstaller**.
- Confirmez la désinstallation.

En outre, vous devez supprimer l'appareil du compte Avira Free Android Security de la console Web.

- Ouvrez la console Web Avira.
- Cliquez sur le lien **Compte** de la barre de titre.
- Accédez à la gestion des appareils et ouvrez le menu déroulant **Appareils disponibles**.
- Sélectionnez l'appareil duquel vous souhaitez supprimer l'application Avira Free Android Security.
- Cliquez sur **Supprimer l'appareil** afin de supprimer l'appareil de votre compte.

Réinstallation

Une fois tous vos appareils désinstallés, vous ne pouvez plus accéder à la console Web Avira.

Vous pouvez toutefois réinstaller Avira Free Android Security sur un appareil à l'aide de votre compte de messagerie précédent.

- Accédez à la console Web en utilisant vos anciennes informations de connexion.
- Une fois connecté, vous pouvez modifier votre mot de passe via la section relative à la **gestion des mots de passe**.

  Sélectionnez **Compte > Gestion des mots de passe**, tapez votre nouveau mot de passe et confirmez-le.
- Si vous avez oublié votre mot de passe, cliquez sur le lien **Mot de passe oublié ?** sur la page de connexion.
  - ↳ Nous vous invitons à nous envoyer votre adresse e-mail. Nous vous enverrons ensuite un lien vous permettant de redéfinir votre mot de passe.

Création du compte Android

Pour garder un œil en permanence sur votre smartphone et protéger vos données personnelles à l'aide de diverses fonctions à distance via la console Web, vous devez d'abord créer un compte Avira Free Android Security.

- Ouvrez le Control Center de votre produit Avira.
- Cliquez sur **Control Center > Protection mobile > Android Security**.
  - ↳ La page de téléchargement d'Avira Free Android Security s'affiche.



- Cliquez sur **Télécharger maintenant**.

  ↳ La page Web des applications Google Play Android s'affiche.

  Cliquez sur **Installer**.

  ↳ Vous êtes invité à vous connecter à Google pour télécharger l'application Avira Free Android Security.

  Cliquez sur **Se connecter**.

  Entrez votre adresse e-mail et votre mot de passe.

  Cliquez sur **Se connecter**.

  Sélectionnez l'appareil sur lequel vous souhaitez télécharger Avira Free Android Security.

  Cliquez sur **Installer**.

  ↳ L'application est téléchargée sur votre appareil Android.

- Ouvrez Avira Free Android Security sur votre appareil.

  ↳ Les nouvelles fonctions de l'application vous sont présentées. Ensuite, vous êtes invité à enregistrer votre appareil via l'écran d'enregistrement d'Avira Free Android Security. Pour ce faire, vous pouvez utiliser votre compte Google ou une adresse e-mail créée auprès d'un autre fournisseur.

↳ La page de votre compte s'affiche.

- Entrez vos informations de connexion.
- Appuyez sur **Accepter le CLUF et continuer** pour poursuivre.

  ↳ Vous recevrez un message de confirmation d'Avira pour votre nouveau compte. Ce message de confirmation comprend un lien vous permettant de définir un mot de passe personnel pour vous connecter à la console Web Android.

- Cliquez sur le lien repris dans le message de confirmation pour définir un mot de passe et activer la console Web Android.

  ↳ La console Web vous permet désormais de contrôler à distance vos appareils via la page Web suivante : https://android.avira.com

Création du compte Android en quelques secondes

Pour garder un œil en permanence sur votre smartphone et protéger vos données personnelles à l'aide de diverses fonctions à distance via la console Web, vous devez d'abord créer un compte Avira Free Android Security.

- Ouvrez la page Web Avira Free Android Security.

  ↳ Le lien permettant d'accéder à la page de téléchargement d'Avira Free Android Security s'affiche.

- Cliquez sur le bouton **Se connecter maintenant**.

  ↳ La page de connexion s'affiche.

- Entrez votre adresse Google ou une autre adresse e-mail de votre choix.

  Cliquez sur **Créer un compte**.

  ↳ Avira envoie le message de confirmation à l'adresse spécifiée. Ce message de confirmation comprend un lien vous permettant d'accéder à la console Web d'Avira Free Android Security.

- Cliquez sur le lien repris dans le message de confirmation.

  ↳ Vous accédez à la console Web Avira Free Android Security.

  ↳ La console Web vous permet désormais de contrôler à distance vos appareils via la page suivante : https://android.avira.com

> **Remarque**
> Lorsque vous téléchargez l'application Avira Free Android Security sur votre appareil après vous être enregistré sur la console Web, veillez à utiliser les mêmes informations de connexion sur la page **Votre compte** lors de la configuration.



Connexion à votre compte Android

- Cliquez sur **Control Center > Protection mobile > Android Security**.
  - ↳ La page de téléchargement d'Avira Free Android Security s'affiche.
- Cliquez sur **Se connecter**.
  - ↳ La page de connexion d'Avira Free Android Security s'affiche.
- Entrez votre adresse e-mail enregistrée et votre mot de passe.
- Cliquez sur **Se connecter** pour ouvrir la console Web et accéder à ses fonctions de commande à distance.

12.10 Généralités

12.10.1 Catégories de dangers

Sélection de catégories de dangers étendues (Options disponibles uniquement si le mode expert est activé)

Votre produit Avira vous protège des virus informatiques. En outre, vous avez la possibilité d'effectuer différentes recherches selon les catégories de dangers suivantes.

- Logiciels publicitaires
- Logiciels publicitaires/logiciels espions
- Applications
- Logiciels de commande Backdoor
- Fichiers à extensions déguisées
- Programmes de numérotation payants
- Hameçonnage
- Programmes portant atteinte à la vie privée
- Programmes de blagues
- Jeux
- Logiciels frauduleux
- Logiciels de compression inhabituels

Cliquez sur la case correspondante pour activer le type sélectionné (coché) ou le désactiver (décoché).

Activer tout

Si l'option est activée, tous les types sont activés.

Valeurs par défaut

Ce bouton restaure les valeurs définies par défaut.

> **Remarque**
> Si un type est désactivé, les fichiers identifiés comme type de programme correspondant ne sont plus signalés. En outre, aucune entrée n'est ajoutée au fichier rapport.

12.10.2 Protection étendue

Protection étendue

ProActiv (Option disponible uniquement si le mode expert est activé.)

Activer la fonction ProActiv

Si l'option est activée, les programmes de votre ordinateur sont surveillés et examinés pour savoir s'ils exécutent des actions suspectes. En cas de comportement typique de logiciels malveillants, vous êtes averti par un message. Vous avez la possibilité de bloquer le programme ou de poursuivre son exécution à l'aide de l'option « **Ignorer** ». Sont exclus de la surveillance : les programmes classifiés comme étant dignes de confiance, les programmes signés et dignes de confiance figurant par défaut dans le filtre des applications autorisées, tous les programmes que vous avez ajoutés au filtre des programmes autorisés.

En utilisant la fonction ProActiv, vous vous protégez contre les nouvelles menaces et les menaces inconnues pour lesquelles il n'existe encore aucune définition de virus ni heuristique. La technologie ProActiv, intégrée au composant Protection temps réel, observe et analyse les actions exécutées par des programmes. Le comportement de programmes est examiné à la recherche de modèles d'action typiques d'un logiciel malveillant : type d'action et séquences de l'action. Si un programme a un comportement typique d'un logiciel malveillant, celui-ci est traité et signalé comme un résultat positif de virus : vous avez la possibilité de bloquer l'exécution du programme ou d'ignorer le message et de poursuivre l'exécution du programme. Vous pouvez classer le programme comme étant digne de confiance et l'ajouter ainsi au filtre des programmes autorisés. Vous avez également la possibilité d'ajouter le programme au filtre des programmes à bloquer via l'instruction **Toujours bloquer**.

Pour déterminer s'il s'agit d'un comportement suspect, le composant ProActiv utilise un ensemble de règles mises au point par le centre de recherche sur les logiciels malveillants Avira Malware Research Center. Les ensembles de règles sont alimentés par les bases de données Avira. Pour la saisie d'informations dans les bases de données Avira, ProActiv envoie des informations sur les programmes signalés comme suspects. Au cours de l'installation d'Avira, vous pouvez désactiver la transmission de données aux bases de données Avira.

> **Remarque**
> La technologie ProActiv n'est pas encore disponible sur les systèmes 64 bits.

Protection Cloud (Options disponibles uniquement si le mode expert est activé.)

Activer la protection Cloud

Les empreintes de tous les fichiers suspects sont transmises au Cloud d'Avira pour la détection en ligne dynamique. Les fichiers d'applications sont aussitôt identifiés comme étant sains, contaminés ou inconnus.

Le système de protection Cloud sert de nœud central pour détecter les cyber-attaques à l'encontre de la communauté Avira. Les fichiers auxquels votre PC accède sont comparés avec des modèles de fichiers enregistrés dans le système de Cloud. L'essentiel du travail ayant lieu dans le Cloud, le programme de protection local a besoin de moins de ressources.

Une liste des emplacements d'enregistrement des fichiers ciblés par le logiciels malveillants est établie à chaque **contrôle rapide du système**. Dans cette liste figurent par exemple les processus, les programmes de démarrage et les programmes de services en cours. Une somme de contrôle numérique (« empreinte ») est créée à partir de chaque fichier ; elle est envoyée au système de protection Cloud, pour être ensuite identifiée comme « saine » ou « logiciel malveillant ». Les fichiers de programmes inconnus sont chargés dans le système de protection Cloud en vue de leur analyse.

Confirmer manuellement en cas d'envoi de fichiers suspects à Avira

Vous pouvez contrôler la liste des fichiers suspects qui doivent être envoyés à la protection Cloud et choisir vous-même les fichiers que vous souhaitez charger.

Sous *Applications à bloquer*, vous pouvez ajouter les applications que vous considérez comme nuisibles et qui doivent être bloquées par défaut par Avira ProActiv. Les applications ajoutées ne peuvent pas être exécutées sur votre système informatique. Vous pouvez également ajouter des programmes au filtre des applications à bloquer via les messages de la protection temps réel concernant le comportement suspect d'un programme en utilisant l'option **Toujours bloquer ce programme** .

Applications à bloquer

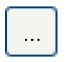
Application

La liste reprend toutes les applications que vous avez classées comme étant nuisibles et que vous avez ajoutées via la configuration ou via les messages du composant ProActiv. Les applications de la liste sont bloquées par Avira ProActiv et ne peuvent pas être exécutées sur votre système informatique. Lors du démarrage d'un programme à bloquer, un message du système d'exploitation s'affiche. Avira ProActiv identifie les applications à bloquer à l'aide du chemin indiqué et du nom de fichier et les bloque indépendamment de leur contenu.

Champ de saisie

Saisissez dans ce champ l'application qui doit être bloquée. Pour identifier l'application, il faut indiquer le chemin complet et le nom de fichier avec son extension.

L'indication de chemin doit soit contenir le lecteur sur lequel se trouve l'application, soit commencer avec une variable d'environnement.



Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner l'application à bloquer.

Ajouter

Le bouton « **Ajouter** » vous permet de reprendre dans la liste des applications à bloquer, l'application indiquée dans le champ de saisie.

Remarque
Les applications nécessaires au fonctionnement du système d'exploitation ne peuvent être ajoutées à la liste.

Supprimer

Le bouton « **Supprimer** » vous permet de supprimer une application sélectionnée de la liste des applications à bloquer.

Sous *Applications à exclure*, sont énumérées les applications qui sont exclues de la surveillance du composant ProActiv : les programmes signés classifiés comme dignes de confiance et figurant par défaut dans la liste, toutes les applications que vous considérez comme étant dignes de confiance et que vous ajoutez dans le filtre des applications : dans la configuration, vous pouvez ajouter des applications à la liste des applications autorisées. Vous pouvez également ajouter des applications via les messages de la protection temps réel concernant le comportement suspect d'un programme, en utilisant l'option **Programme digne de confiance** dans le message de la protection temps réel.

Applications à exclure

Application

La liste contient les applications exclues de la surveillance du composant ProActiv. Dans les paramètres par défaut après l'installation, la liste contient les applications signées de fabricants dignes de confiance. Vous avez la possibilité d'ajouter les applications que vous avez classifiées comme étant dignes de confiance via la configuration ou via les messages de la protection temps réel. Le composant ProActiv identifie les applications à l'aide du chemin, du nom de fichier et du contenu. Un contrôle de contenu est judicieux car il est possible d'ajouter ultérieurement à un programme un code malveillant via des modifications telles que des mises à jour. Le **type** indiqué vous permet de déterminer la manière dont le contenu doit être contrôlé : avec le type « *Contenu* », les applications indiquées avec le chemin et le nom de fichier sont examinées pour voir si le contenu du fichier ne présente pas des modifications, avant d'être exclues de la surveillance par le composant ProActiv. En cas de modification du contenu du fichier, l'application est à nouveau surveillée par le composant ProActiv. Avec le type « *Chemin* », il n'y a pas de contrôle du contenu

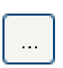
avant que l'application ne soit exclue de la surveillance effectuée par la protection temps réel. Pour changer le type d'exclusion, cliquez sur le type affiché.

Avertissement
Utilisez le type *Chemin* uniquement dans des cas exceptionnels. Une mise à jour peut permettre d'ajouter un code malveillant à une application. L'application à l'origine inoffensive devient alors un logiciel malveillant.

Remarque
Quelques applications dignes de confiance comme p. ex. tous les composants d'application de votre produit Avira, sont exclus par défaut d'une surveillance par le composant ProActiv, mais ne figurent pas sur la liste.

Champ de saisie

Dans ce champ, vous indiquez l'application devant être exclue de la surveillance par le composant ProActiv. Pour identifier l'application, il faut indiquer le chemin complet et le nom de fichier avec son extension. L'indication de chemin doit soit contenir le lecteur sur lequel se trouve l'application, soit commencer avec une variable d'environnement.



Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner l'application à exclure.

Ajouter

Le bouton « **Ajouter** » vous permet de reprendre dans la liste des applications à exclure, l'application indiquée dans le champ de saisie.

Supprimer

Le bouton « **Supprimer** » vous permet de supprimer une application sélectionnée de la liste des applications à exclure.

12.10.3 Mot de passe

Vous pouvez protéger votre produit Avira dans diverses zones par un mot de passe. Si un mot de passe a été attribué, vous devez saisir ce mot de passe à chaque fois que vous voulez ouvrir la zone protégée.

Mot de passe

Saisir le mot de passe

Saisissez ici le mot de passe de votre choix. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*). Vous pouvez saisir 20 caractères au maximum. Si le mot de passe est indiqué une

fois, le programme refuse l'accès en cas de saisie d'un mot de passe erroné. Un champ vide signifie « Aucun mot de passe ».

Confirmation

Saisissez ici de nouveau le mot de passe indiqué ci-dessus pour le confirmer. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*).

Remarque
Le mot de passe est sensible à la casse.

Zones protégées par mot de passe (options disponibles uniquement si le mode expert est activé.)

Votre produit Avira peut protéger diverses zones par mot de passe. En cliquant sur la case correspondante, la demande de mot de passe pour les diverses zones peut être désactivée et activée à volonté.

Zone protégée par mot de passe	Fonction
Control Center	Si l'option est activée, le mot de passe défini est nécessaire pour le démarrage du Control Center.
Activer / désactiver la protection temps réel	Si l'option est activée, le mot de passe défini est nécessaire pour activer et désactiver la protection temps réel Avira.
Activer / désactiver la protection e-mail	Si l'option est activée, le mot de passe défini est nécessaire pour activer et désactiver la protection e-mail.
Activer / désactiver FireWall	Si l'option est activée, le mot de passe défini est nécessaire pour activer et désactiver le FireWall.
Activer / désactiver la protection Web	Si l'option est activée, le mot de passe défini est nécessaire pour activer et désactiver la protection Web.
Activer / désactiver la Navigation sécurisée	Si l'option est activée, le mot de passe défini est nécessaire pour activer et désactiver le contrôle parental.



Quarantaine	Si l'option est activée, le mot de passe défini est nécessaire pour activer et désactiver toutes les zones du gestionnaire de quarantaines. En cliquant sur la case correspondante, la demande de mot de passe peut être désactivée et activée à volonté.
Restauration des objets concernés	Si l'option est activée, le mot de passe défini est nécessaire pour restaurer un objet.
Nouveau contrôle des objets concernés	Si l'option est activée, le mot de passe défini est nécessaire pour contrôler à nouveau un objet.
Propriétés des objets concernés	Si l'option est activée, le mot de passe défini est nécessaire pour afficher les propriétés d'un objet.
Suppression des objets concernés	Si l'option est activée, le mot de passe défini est nécessaire pour supprimer un objet.
Envoyer un e-mail à Avira	Si l'option est activée, le mot de passe défini est nécessaire pour envoyer un objet à l'Avira Malware Research Center pour contrôle.
Copie des objets concernés	Si l'option est activée, le mot de passe défini est nécessaire pour copier les objets concernés.
Ajout et modification des tâches	Si l'option est activée, le mot de passe défini est nécessaire pour ajouter et modifier des tâches dans le planificateur.
Configuration	Si l'option est activée, la configuration du programme n'est possible qu'après saisie du mot de passe défini.
Installation / désinstallation	Si l'option est activée, le mot de passe défini est nécessaire pour installer et désinstaller le programme.

12.10.4 Sécurité

Options disponibles uniquement si le mode expert est activé.

Autorun

Bloquer la fonction Autorun

Si l'option est activée, l'exécution de la fonction Autorun de Windows est bloquée sur tous les lecteurs intégrés comme les clés USB, les lecteurs de CD et DVD, les lecteurs réseau. Avec la fonction Autorun de Windows, les fichiers sur des supports de données ou sur des lecteurs réseau sont immédiatement lus lors de l'insertion ou de la connexion. Ainsi, les fichiers peuvent être démarrés et reproduits automatiquement. Cette fonctionnalité implique toutefois un risque élevé pour la sécurité, car des logiciels malveillants ou programmes indésirables peuvent être installés en cas de démarrage automatique des fichiers. La fonction Autorun est particulièrement critique pour les clés USB car les données d'une clé USB peuvent constamment changer.

Exclure les CD et DVD

Si l'option est activée, la fonction Autorun est autorisée sur les lecteurs de CD et DVD.

Avertissement
Ne désactivez la fonction Autorun pour les lecteurs de CD et DVD que si vous êtes certain d'utiliser uniquement des supports de données fiables.

Protection système

Protéger le fichier hôte Windows des modifications

Si cette option est activée, le fichier hôte Windows est protégé en écriture. Il n'est plus possible de manipuler le fichier. Les logiciels malveillants ne sont plus capables, par exemple, de vous rediriger sur des pages Internet non souhaitées. Cette option est activée par défaut.

Protection du produit

Remarque
Les options de protection du produit ne sont pas disponibles si la protection temps réel n'a pas été installée lors d'une installation personnalisée.

Protéger les processus d'un arrêt non souhaité

Si l'option est activée, tous les processus du programme sont protégés d'un arrêt non souhaité par des virus et des logiciels malveillants ou d'un arrêt « incontrôlé » par un utilisateur, par ex. via le gestionnaire des tâches. Cette option est activée par défaut.

Protection étendue des processus

Si l'option est activée, tous les processus du programme sont protégés par des méthodes avancées contre un arrêt non souhaité. La protection étendue des processus utilise beaucoup plus de ressources que la protection simple des processus. L'option est activée par défaut. Un redémarrage de l'ordinateur est nécessaire pour désactiver l'option.

Remarque
La protection de processus n'est pas disponible sous Windows XP 64 bits !

Avertissement
Si la protection des processus est activée, des problèmes d'interaction peuvent survenir avec d'autres logiciels. Désactivez la protection des processus dans ces cas.

Protéger les fichiers et entrées de Registre de toute manipulation

Si l'option est activée, toutes les entrées de Registre du programme, ainsi que tous les fichiers (fichiers binaires et de configuration) sont protégés contre toute manipulation. La protection contre la manipulation comprend la protection contre l'accès en écriture, en suppression et partiellement en lecture aux entrées de Registre ou aux fichiers du programme, par l'utilisateur ou des programmes-tiers. Pour activer l'option, il est nécessaire de redémarrer l'ordinateur.

Avertissement
Veuillez noter que si l'option est désactivée, il se peut que la réparation des ordinateurs contaminés par certains types de logiciels malveillants échoue.

Remarque
Si l'option est activée, les modifications de la configuration ne sont possibles que via l'interface utilisateur, de même que la modification des tâches de contrôle ou de mise à jour.

Remarque
La protection des fichiers et des entrées de Registre n'est pas disponible sous Windows XP 64 bits !

12.10.5 WMI

Options disponibles uniquement si le mode expert est activé.

Prise en charge de Windows Management Instrumentation (WMI)

Windows Management Instrumentation est une technologie de gestion Windows de base qui permet d'accéder en lecture et en écriture aux paramètres d'ordinateurs Windows, localement et à distance, au moyen de langages de script et de programmation. Votre produit Avira prend en charge WMI et met à disposition d'une interface, les données (informations sur l'état, données statistiques, rapports, tâches planifiées, etc.) ainsi que les

événements . WMI vous donne la possibilité de consulter les données d'exploitation du programme.

Activer la prise en charge WMI

Si l'option est activée, vous avez la possibilité de consulter les données d'exploitation du programme via WMI.

12.10.6 Événements

Options disponibles uniquement si le mode expert est activé.

Limiter la taille de la base de données d'événements

Limiter la taille à n entrées maximum

Si l'option est activée, le nombre maximum d'entrées dans la base de données d'événements peut être limité à une taille définie ; les valeurs autorisées sont : 100 à 10 000 entrées. Si le nombre d'entrées saisies est dépassé, les saisies les plus anciennes sont supprimées.

Supprimer tous les événements de plus de n jour(s)

Si l'option est activée, les événements sont supprimés de la base de données d'événements après un certain nombre de jours ; les valeurs autorisées sont : 1 à 90 jours. Cette option est définie par défaut sur une valeur de 30 jours.

Pas de limitation

Si l'option est activée, la taille de la base de données d'événements n'est pas limitée. Toutefois, 20 000 entrées au maximum sont affichées sur l'interface du programme sous Événements.

12.10.7 Rapports

Options disponibles uniquement si le mode expert est activé.

Limiter les rapports

Limiter le nombre maximum à n unités

Si cette option est activée, le nombre maximum de rapports peut être limité ; les valeurs autorisées sont : 1 à 300. Si le nombre indiqué est dépassé, les rapports les plus anciens sont supprimés.

Supprimer tous les rapports de plus de n jour(s)

Si cette option est activée, les rapports sont supprimés automatiquement après un certain nombre de jours ; valeurs autorisées : 1 à 90 jours. Cette option est définie par défaut sur une valeur de 30 jours.

Pas de limitation

Si cette option est activée, le nombre de rapports n'est pas limité.

12.10.8 Répertoires

Options disponibles uniquement si le mode expert est activé.

Chemin temporaire

Utiliser le paramètre du système

Si cette option est activée, les paramètres du système sont utilisés pour le traitement des fichiers temporaires.

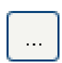
> **Remarque**
> Pour savoir où votre système enregistre les fichiers temporaires, sur Windows XP par exemple, allez sous : **Démarrer > Panneau de configuration > Performances et maintenance > Système >** onglet « **Avancé** » > bouton « **Variables d'environnement** ». Les variables temporaires (`TEMP`, `TMP`) pour l'utilisateur connecté et pour les variables du système (`TEMP`, `TMP`) sont visibles ici avec leurs valeurs respectives.

Utiliser le répertoire suivant

Si l'option est activée, c'est le chemin indiqué dans le champ de saisie qui est utilisé.

Champ de saisie

Entrez dans ce champ de saisie le chemin sous lequel le programme doit enregistrer les fichiers temporaires.



Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner le chemin temporaire souhaité.

Par défaut

Ce bouton restaure le répertoire prédéfini pour le chemin temporaire.

12.10.9 Avertissement sonore

Options disponibles uniquement si le mode expert est activé.

En cas de détection d'un virus ou d'un logiciel malveillant par le scanner ou la protection temps réel, un signal sonore d'avertissement retentit dans le mode d'action interactif. Vous pouvez désactiver ou activer le signal sonore d'avertissement, ou sélectionner un autre fichier WAVE comme signal sonore d'avertissement.

> **Remarque**
> Le mode d'action du scanner se règle dans la configuration sous Sécurité PC > Scanner > Recherche > Action si résultat positif. Le mode d'action de la protection temps réel se règle dans la configuration sous Sécurité PC > Protection temps réel > Recherche > Action si résultat positif.

Pas d'avertissement

Si l'option est activée, aucun avertissement sonore ne se produit lors de la détection d'un virus par le scanner ou la protection temps réel.

Diffuser par le haut-parleur du PC (uniquement en mode interactif)

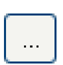
Si l'option est activée, un avertissement sonore se produit à l'aide d'un signal sonore d'avertissement par défaut, lors de la détection d'un virus par le scanner ou la protection temps réel. Le signal sonore d'avertissement est diffusé par le haut-parleur interne du PC.

Utiliser le fichier WAVE suivant (uniquement en mode interactif)

Si l'option est activée, un avertissement sonore se produit à l'aide du fichier WAVE sélectionné, en cas de détection d'un virus par le scanner ou la protection temps réel. Le fichier WAVE sélectionné est diffusé par un haut-parleur externe raccordé.

Fichier WAVE

Dans ce champ de saisie, vous pouvez saisir le nom et le chemin correspondant d'un fichier audio de votre choix. Le signal sonore d'avertissement par défaut du programme est indiqué comme préréglage.



Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner le fichier souhaité à l'aide de l'explorateur de fichiers.

Test

Ce bouton sert à tester le fichier WAVE sélectionné.

12.10.10 Avertissements

Pour certains événements, votre produit Avira affiche des notifications sur le Bureau (slide-up), pour vous informer de dangers et de la réussite ou de l'échec de l'exécution de programmes, p. ex. l'exécution d'une mise à jour. Sous **Avertissements**, vous pouvez activer ou désactiver la notification de certains événements.

En cas de notifications affichées sur le Bureau, vous avez la possibilité de désactiver directement la notification dans le slide-up. Vous pouvez annuler la désactivation de la notification dans la fenêtre de configuration **Avertissements**.

Mise à jour



Avertissement si la dernière mise à jour date de plus de n jour(s)

Dans ce champ, vous pouvez saisir le nombre de jours maximum qui doit s'être écoulé depuis la dernière mise à jour. Si cette période est dépassée, une icône rouge s'affiche dans le Control Center sous État pour l'état de mise à jour.

Afficher un avertissement si le fichier de définitions des virus est obsolète

Si l'option est activée, vous recevez un message d'avertissement en cas de fichier de définitions des virus obsolète. À l'aide de l'option « Avertissement si la dernière mise à jour date de plus de n jour(s) », vous pouvez configurer l'intervalle avant l'avertissement.

Avertissements / remarques dans les situations suivantes

Une connexion par modem est utilisée

Si l'option est activée, une notification s'affiche sur le Bureau pour vous avertir lorsqu'un programme de numérotation établit sur votre ordinateur une connexion par téléphone ou par réseau RNIS. Le programme de numérotation risque d'être un numéroteur inconnu et indésirable qui établit une connexion payante. (Voir Catégories de dangers : programmes de numérotation payants)

Les fichiers ont été actualisés avec succès

Si l'option est activée, une notification s'affiche sur le Bureau lorsqu'une mise à jour a réussi et que les fichiers ont été actualisés.

Échec de la mise à jour

Si l'option est activée, une notification s'affiche sur le Bureau lorsqu'une mise à jour a échoué : la connexion au serveur de téléchargement n'a pas pu être établie ou les fichiers de mise à jour n'ont pas pu être installés.

Aucune mise à jour n'est nécessaire

Si l'option est activée, une notification s'affiche sur le Bureau lorsqu'une mise à jour a été lancée sans qu'il soit toutefois nécessaire d'installer des fichiers car votre programme est à jour.

Edition du 2ème trimestre 2013.



live *free*.™

Avira Operations GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang
L'Allemagne

Téléphone : +49 7542-500 0
Fax : +49 7542-500 3000
Internet: www.avira.fr